Part No. 202086-C
May 2001

4401 Great America Parkway
Santa Clara, CA 95054

Reference for the Passport 1000 Series Command Line Interface Release 2.1

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. May 2001.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

HThe software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Accelar, Bay Networks, and Passport are registered trademarks.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its

own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface 27

Before you begin 27
Text conventions 28
Related publications 29
Hard-copy technical manuals 31
How to get help 32

Chapter 1
Passport basics 33

Management tools 34
- Device Manager 34
- Boot Monitor command line interface 35
- Run-Time command line interface 35
- Passport Configuration Page 35

Boot sequence 36
- Stage 1: Boot monitor image load 36
- Stage 2: Boot configuration load 36
- Stage 3: Run-time image load 37
- Stage 4: Switch configuration load 38

Flash/PCMCIA file system 40
- Flash memory organization 40
  - Boot Flash 40
  - System Flash (flash:) 41
  - PCMCIA (pcmcia:) 41
- File types 41
  - Executables 42
  - Log files 42
  - Configuration files 42

Script files 42
Trace logs 43
Devices and file names 43
System Flash and PCMCIA file names 43
Reserved devices 44
File system commands 45
Format 46
Directory 46
Copy 48
Copy script file to running config 49
Delete 50
Squeeze 51
Recover 51
Passport access levels and passwords 52
Telnet and console passwords 53
CLI commands to change the console/Telnet password 54

Chapter 2
Boot Monitor command line interface 55

System and station requirements 55
Accessing the Boot Monitor CLI 56
Boot monitor command list 56
Boot commands 59
File and device management commands 60
Help commands 62
History commands 62
IP command 63
Ping command 65
Show command 67
Quit command 67

Chapter 3
Run-Time CLI description 69

System and station requirements 69
General usage 70

Passwords . . . 71
Navigating through the CLI . . . 71
Getting help . . . 73
Port numbers and IP addresses . . . 73
Specifying port numbers . . . 73
Specifying IP addresses and subnet masks . . . 75
Accessing the Run-Time CLI . . . 76
Run-time command list tree . . . 76
Navigation commands . . . 78
General commands . . . 78
Boot command . . . 79
Boot using a configuration script file . . . 80
Clear commands . . . 80
Date command . . . 81
Help command . . . 81
History commands . . . 84
Login/exit/logout/quit commands . . . 85
Ping and pingipx commands . . . 85
Reset command . . . 86
Traceroute command . . . 87
File and device management commands . . . 88
Copying a script file to a running configuration . . . 91
Accessing files using the standby SSF module . . . 92
Test commands . . . 92
show test commands . . . 93
show test artable command . . . 93
show test fabric command . . . 93
show test loopback command . . . 94
Trace commands . . . 94
show trace commands . . . 95
show trace file command . . . 95
show trace level command . . . 96

Chapter 4
Configuring switch management 97

show config command 97
show tech command 100
CLI management commands 101
config cli commands 101
show cli commands 103
show cli info command 103
show cli who command 104
config cli password commands 104
show cli password command 105
Log commands 105
config log commands 106
show log commands 107
show log file command 107
show log level command 108
RMON commands 109
config rmon commands 109
show rmon command 109
config setdate command 110
System commands 110
Access policy commands 110
config sys commands 111
config sys access-policy commands 111
config sys access-policy policy commands 111
show sys access-policy info command 113
config sys set action commands 114
config sys set flags commands 115
Other config sys set commands 117
show sys commands 119
show sys community command 119
show sys diag info command 120
show sys info command 120
show sys perf command 121
show sys sw command 121

config sys link-flap-detect commands 122
Syslog commands 123
config sys syslog commands 123
show commands 125
show sys syslog general info command 125
show sys syslog host info command 125
web-server commands 125
config web-server commands 126
show web-server command 126

Chapter 5
Configuring layer 2 features 127

Port commands 127
config ethernet ports commands 127
show ports commands 129
show ports error collision command 130
show ports error main command 131
show ports error extended command 132
show ports info config command 133
show ports info interface command 134
show ports stats bridging command 135
show ports stats interface main command 136
show ports stats interface extended command 137
show ports info vlans command 138
config ethernet ports ip commands 140
config ethernet <ports> unknown-mac-discard commands 140
RADIUS commands 142
config radius commands 142
Port Mirroring commands 144
config mirror commands 145
show mirrorinfo command 145
MLT commands 146
config mlt commands 146
show mlt commands 147
show mlt error collision command 147

show mlt error main command 148
show mlt info command 148
show mlt stats command 149
Spanning tree group commands 149
config stg commands 150
config ethernet ports stg commands 151
show stg commands 152
show stg info config command 153
show stg info status command 153
show ports info stg main command 154
show ports info stg extended command 155
show ports stats stg command 156
VLAN commands 157
config vlan create commands 157
config vlan general commands 159
show vlan general commands 161
show vlan info command 161
show vlan info basic command 161
show vlan info advance command 162
show vlan info fdb-entry command 162
show vlan info fdb-filter command 163
show vlan info fdb-static command 163
show vlan info ports command 164
show vlan info srcmac command 164
config vlan fdb (forwarding database) commands 165
config vlan igmp-snoop commands 168
show vlan igmp-snoop commands 171
show vlan info snoop command 171
show vlan igmp-snoop access-list command 172
show vlan igmp-snoop all-access-list command 173
show vlan igmp-snoop groups command 173
show vlan igmp-snoop senders info 173
show vlan igmp-snoop static 174
config vlan static-mcastmac 174

Chapter 6
Configuring layer 3 protocol features 177

IP routing commands 177
config ip commands 178
show ip commands 180
show ip forwarding command 180
show ip interface command 180
show ip route-discovery command 181
show ip route info command 181
config ip diffserv-rule commands 182
show ip diffserv command 184
ethernet ports ip commands 185
config ethernet ports ip command 185
show ports info ip 186
vlan ip commands 186
config vlan ip command 186
show vlan info ip command 187
IP ARP commands 188
config ip arp commands 189
config ip arp static-mcastmac 190
show ip arp commands 191
show ip arp info command 191
ethernet ip arp commands 192
config ethernet ip arp command 193
show ports info arp command 193
vlan ip arp general commands 194
config vlan ip arp command 194
show vlan info arp command 195
DHCP relay commands 196
config ip dhcp-relay commands 197
show ip dhcp commands 197
show ip dhcp fwd-path command 198
show ip dhcp counters command 198
config ethernet ip dhcp-relay commands 198
show port dhcp commands 199

show ports info dhcp command 199
show ports stats dhcp 200
config vlan ip dhcp-relay commands 201
show vlan info dhcp command 202
UDP commands 203
config ip udpfwd protocol command 203
config ip udpfwd portfwdlist commands 204
config ip udpfwd interface commands 205
show ip udpfwd commands 205
show ip udpfwd interface info command 205
show ip udpfwd portfwd info command 206
show ip udpfwd portfwdlist info command 206
show ip udpfwd protocol info command 206
IP Static Routing Table Manager 207
RIP commands 208
config ip rip commands 208
show ip rip commands 210
show ip rip info 210
show ip rip interface 210
config ethernet port ip rip commands 211
show ports info rip command 214
config vlan ip rip commands 215
show vlan info rip command 217
OSPF commands 218
config ip ospf commands 218
config ip ospf command 219
config ip ospf host-route command 220
config ip ospf interface commands 221
config ip ospf area 222
config ip ospf area range commands 223
config ip ospf area virtual-interface command 224
show ip ospf commands 225
show ip ospf area command 225
show ip ospf ase command 226
show ip ospf default-metric command 226

show ip ospf host-route command 227
show ip ospf ifstats command 227
show ip ospf info command 227
show ip ospf interface command 228
show ip ospf int-timers command 229
show ip ospf lsdb command 230
show ip ospf neighbors commands 230
show ip ospf range command 231
show ip ospf stats command 231
configure ethernet port ip ospf commands 232
show port ospf commands 234
show ports error ospf command 234
show ports info ospf command 234
show ports stats ospf main command 235
show ports stats ospf extended command 236
config vlan ip ospf commands 237
show vlan info ospf command 239
VRRP commands 240
config ip vrrp commands 240
config ethernet port ip vrrp commands 241
show port vrrp commands 242
show ports info vrrp main command 242
show ports info vrrp extended command 243
show ports stats vrrp command 243
config vlan ip vrrp commands 244
show vlan vrrp commands 245
show vlan info vrrp main command 245
show vlan info vrr extended command 245
show ip vrrp commands 245
show ip vrrp info command 245
show ip vrrp stats command 246
IP multicast commands 246
config ip mroute commands 246
show ip mroute commands 247
show ip mroute interface command 247

show ip mroute next-hop command 247
show ip mroute route 248
show ports stats routing command 248
DVMRP commands 249
config ip dvmrp commands 249
config ip dvmrp command 250
config ip dvmrp interface command 251
show ip dvmrp commands 251
show ip dvmrp info command 251
show ip dvmrp interface command 252
show ip dvmrp neighbor command 252
show ip dvmrp next-hop command 253
show ip dvmrp route command 253
config ethernet ip dvmrp commands 254
show ports info dvmrp command 255
config vlan ip dvmrp commands 256
show vlan info dvmrp command 256
Layer 3 IGMP commands 257
config ip l3 igmp commands 257
config ip l3-igmp interface 257
show ip l3 igmp commands 258
show ip l3-igmp cache command 258
show ip l3-igmp group command 259
show ip l3-igmp interface 259
config ethernet ip l3-igmp commands 260
show ports info l3-igmp command 261
config vlan ip l3-igmp commands 261
show vlan info l3-igmp command 263
IPX commands 263
config ipx commands 264
config vlan ipx commands 266
config ipx set commands 267
config ipx static-route commands 268
config ipx rip commands 268
config ipx rip default command 269

config ipx rip info command 269
config ipx rip command 270
config ipx sap commands 270
config ipx sap info command 270
config ipx sap default 271
config ipx sap command 272
show ipx commands 272
show ipx config command 273
show ipx default command 273
show ipx route command 273
show ipx sap command 274
show ipx stats command 274
show vlan info ipx command 275

Chapter 7
Configuring IP flow, policies, and filters 277

IP flow commands 277
config ip flow commands 278
show ip flow command 278
IP policies 279
config ip policy commands 279
config ip policy info command 280
config ip policy addrlist command 280
config ip policy netlist command 281
config ip policy ospf command 282
config ip policy ospf accept command 282
config ip policy ospf announce command 284
config ip policy rip commands 285
config ip policy rip accept commands 286
config ip policy rip announce command 287
show ip policy commands 289
show ip policy addrlist info command 289
show ip policy netlist info command 290
show ip policy ospf accept info command 291
show ip policy ospf accept lists command 291

show ip policy ospf accept match network command 292
show ip policy ospf announce info command 292
show ip policy ospf announce lists command 292
show ip policy ospf announce match network command 292
show ip policy rip accept info command 293
show ip policy rip accept lists command 293
show ip policy rip accept match network command 293
show ip policy rip announce info command 293
show ip policy rip announce lists command 294
show ip policy rip announce match network command 294
IP filters 294
config ip filter commands 295
config ip traffic-filter commands 295
config ip traffic-filter create commands 296
config ip traffic-filter filter commands 296
config ip traffic-filter filter action command 297
config ip traffic-filter filter match commands 299
config ip traffic-filter global-set commands 300
config ip traffic-filter set commands 300
config ethernet ip traffic-filter commands 301
show ip traffic-filter commands 301
show ip traffic-filter active command 301
show ip traffic-filter destination command 302
show ip traffic-filter disabled command 302
show ip traffic-filter enabled command 302
show ip traffic-filter global command 302
show ip traffic-filter info global-set command 303
show ip traffic-filter info list command 303
show ip traffic-filter interface command 303
show ip traffic-filter log-interval command 303
show ip traffic-filter source command 303
show ip traffic-filter stats command 304

Chapter 8
Monitor commands 305

Appendix A
CLI command list 309

Appendix B
Port numbering and MAC address assignment 343

Port numbering 343
MAC address assignment 344
Base MAC address 345
Physical MAC addresses 346
Virtual MAC addresses 347
Index 349

Figures

Figure 1 Passport 1200 directory flash command example 47
Figure 2 Passport 1100 directory flash command example 48
Figure 3 copy command 49
Figure 4 directory flash command 49
Figure 5 directory command output 62
Figure 6 ip command output 64
Figure 7 ping command output 66
Figure 8 Passport 1200 slot and port numbering 74
Figure 9 Partial Run-Time CLI tree 77
Figure 10 Passport 1000 Series online Help 82
Figure 11 help command output in the Run-Time CLI 83
Figure 12 help config command output 84
Figure 13 history command output 85
Figure 14 ping command output 86
Figure 15 traceroute command output 87
Figure 16 file and device management commands output 90
Figure 17 show test artable command output 93
Figure 18 show test fabric command output 94
Figure 19 show test loopback command output 94
Figure 20 show trace file command output 96
Figure 21 show trace level command output 96
Figure 22 show config command output 98
Figure 23 show tech command output 101
Figure 24 config cli info command output 103
Figure 25 show cli info command output 103
Figure 26 show cli who command output 104
Figure 27 config cli password info command output 105
Figure 28 show cli password command output 105
Figure 29 config log command output 106

Figure 30 show log file tail command output 108
Figure 31 show log level command output 108
Figure 32 show rmon command output 109
Figure 33 config sys access-policy policy command output 113
Figure 34 deny access command output 113
Figure 35 show sys access-policy info command output 114
Figure 36 config sys set action command output 115
Figure 37 config sys set flags info command output 116
Figure 38 config sys set info command output 118
Figure 39 config sys set snmp info command output 119
Figure 40 show sys community command output 119
Figure 41 show sys diag info command output 120
Figure 42 show sys info command output 120
Figure 43 show sys perf command output 121
Figure 44 show sys sw command output 122
Figure 45 config sys link-flap-detect info command output 123
Figure 46 config sys syslog command output 124
Figure 47 show sys syslog general info command output 125
Figure 48 show web-server command output 126
Figure 49 config ethernet info command output 129
Figure 50 show ports error collision command output 131
Figure 51 show ports error main command output 132
Figure 52 show ports error extended command output 133
Figure 53 show ports info config command output 134
Figure 54 show ports info interface command output 135
Figure 55 show ports stats bridging command output 136
Figure 56 show ports stats interface main command output 137
Figure 57 show ports stats interface extended command output 138
Figure 58 show ports info vlans command output 139
Figure 59 show mirrorinfo command output 146
Figure 60 config mlt info command output 147
Figure 61 config mlt add info command output 147
Figure 62 show mlt error collision command output 148
Figure 63 show mlt error main command output 148
Figure 64 show mlt info command output 149

Figure 65 show mlt stats command output 149
Figure 66 config stg info command output 151
Figure 67 config ethernet stg info command output 152
Figure 68 show stg info config command output 153
Figure 69 show stg info status command output 154
Figure 70 show ports info stg main command output 155
Figure 71 show ports info stg extended command output 156
Figure 72 show ports stats stg command output 157
Figure 73 config vlan create info command output 158
Figure 74 config vlan info command output 160
Figure 75 config vlan ports info command output 160
Figure 76 config vlan srcmac info command output 160
Figure 77 show vlan info basic command output 161
Figure 78 show vlan info advance command output 162
Figure 79 show vlan info fdb-entry command output 163
Figure 80 show vlan info ports command output 164
Figure 81 show vlan info srcmac command output 165
Figure 82 config vlan fdb-entry info command output 167
Figure 83 config vlan fdb-filter info command output 167
Figure 84 config vlan fdb filter notallowfrom info command output 167
Figure 85 config vlan fdb-static info command output 168
Figure 86 config vlan igmp-snoop info command output 171
Figure 87 show vlan info snoop command output 172
Figure 88 show vlan igmp-snoop access-list command output 172
Figure 89 show vlan igmp-snoop groups command output 173
Figure 90 show vlan igmp-snoop senders info command output 174
Figure 91 show vlan igmp-snoop static command output 174
Figure 92 config ip info command output 179
Figure 93 config ip forwarding info command output 179
Figure 94 config ip route-discovery info command output 179
Figure 95 config ip static-route info command output 180
Figure 96 show ip forwarding command output 180
Figure 97 show ip interface command output 181
Figure 98 show ip route-discovery command 181
Figure 99 show ip route info command output 182

Figure 100 show ip diffserv command output 184
Figure 101 config ethernet ip info command output 186
Figure 102 show ports info ip command output 186
Figure 103 config vlan ip info command output 187
Figure 104 show vlan info ip command output 188
Figure 105 config ip arp info command output 190
Figure 106 show ip arp info command output 192
Figure 107 config ethernet ip arp-response info command output 193
Figure 108 config ethernet ip proxy info command 193
Figure 109 show ports info arp command output 194
Figure 110 config vlan ip proxy info command output 195
Figure 111 config vlan ip resp info command output 195
Figure 112 show vlan info arp command output 196
Figure 113 config ethernet ip dhcp-relay info command output 199
Figure 114 show ports info dhcp command output 200
Figure 115 show ports stats dhcp command output 201
Figure 116 config vlan ip dhcp-relay info command output 202
Figure 117 show vlan info dhcp command output 203
Figure 118 show ip udpfwd interface info command output 206
Figure 119 show ip udpfwd portfwd info command output 206
Figure 120 show ip udpfwd protocol info command output 207
Figure 121 show ip route info command output 208
Figure 122 config ip rip info command output 209
Figure 123 show ip rip info command output 210
Figure 124 show ip rip interface command output 211
Figure 125 config ethernet ip rip info command output 213
Figure 126 show ports info rip command output 215
Figure 127 config vlan ip rip info command output 217
Figure 128 show vlan info rip command output 218
Figure 129 config ip ospf info command output 220
Figure 130 config ip ospf area info command output 223
Figure 131 show ip ospf area command output 225
Figure 132 show ip ospf ase command output 226
Figure 133 show ip ospf default-metric command output 226
Figure 134 show ip ospf ifstats command output 227

Figure 135 show ip ospf info command output 228
Figure 136 show ip ospf interface command output 229
Figure 137 show ip ospf int-timers command output 229
Figure 138 show ip ospf lsdb command output 230
Figure 139 show ospf neighbors command output 230
Figure 140 show ip ospf range command output 231
Figure 141 show ip ospf stats command output 231
Figure 142 config ethernet ip ospf info command output 233
Figure 143 show ports error ospf command output 234
Figure 144 show ports info ospf command output 235
Figure 145 show ports stats ospf main command output 236
Figure 146 show ports stats ospf extended command output 237
Figure 147 config vlan ip ospf info command output 239
Figure 148 show vlan info ospf command output 239
Figure 149 config ethernet ports ip vrrp info command output 242
Figure 150 show ports info vrrp main command output 243
Figure 151 show ports info vrrp extended command output 243
Figure 152 show ip mroute interface command output 247
Figure 153 show ip mroute next-hop command output 247
Figure 154 show ip mroute route command output 248
Figure 155 show ports stats routing command output 249
Figure 156 config ip dvmrp info command output 250
Figure 157 show ip dvmrp info command output 252
Figure 158 show ip dvmrp interface command 252
Figure 159 show ip dvmrp neighbor command output 253
Figure 160 show ip dvmrp next-hop command output 253
Figure 161 show ip dvmrp route command output 254
Figure 162 config ethernet ip dvmrp info command output 254
Figure 163 show ports info dvmrp command output 255
Figure 164 config vlan ip dvmrp info command output 256
Figure 165 show vlan info dvmrp command output 257
Figure 166 show ip l3-igmp cache command output 258
Figure 167 show ip l3-igmp group command output 259
Figure 168 show ip l3-igmp interface command output 259
Figure 169 config ethernet ip l3-igmp info command output 260

Figure 170 show ports info l3-igmp command output 261
Figure 171 config vlan ip l3-igmp info command output 262
Figure 172 show vlan info l3-igmp command output 263
Figure 173 config ipx info command output 266
Figure 174 config ipx forwarding info command output 266
Figure 175 config ipx set info command output 267
Figure 176 config ipx static-route info command output 268
Figure 177 config ipx rip info command output 269
Figure 178 config ipx sap info command output 271
Figure 179 show ipx default command output 273
Figure 180 show ipx stats command output 274
Figure 181 config ip flow command output 278
Figure 182 show ip flow command output 279
Figure 183 config ip policy addrlist info command output 280
Figure 184 config ip policy netlist info command output 281
Figure 185 config ip policy ospf accept info command output 283
Figure 186 config ip policy ospf announce info command output 285
Figure 187 config ip policy rip accept info command output 287
Figure 188 config ip policy rip announce info command output 289
Figure 189 show ip policy addrlist info command output 290
Figure 190 show ip policy addrlist info id 1 command output 290
Figure 191 show ip policy netlist info command output 291
Figure 192 show ip policy netlist info id 1 command output 291
Figure 193 config ip traffic-filter info command output 295
Figure 194 config ip traffic-filter filter info command output 297
Figure 195 config ip traffic-filter filter action info command output 298
Figure 196 monitor mlt stats interface utilization command output 306
Figure 197 monitor ports stats interface utilization command output 307
Figure 198 Passport 1200 slots 343
Figure 199 Passport 1100 slots 344
Figure 200 Port numbering on I/O modules 344

Tables

Table 1 Boot monitor parameters 37
Table 2 Command arguments and meaning 44
Table 3 Passport file system commands 45
Table 4 Passport directory flags 46
Table 5 Access levels and default login names and passwords 52
Table 6 Login and password default values 53
Table 7 Boot Monitor CLI commands 57
Table 8 Boot Monitor CLI boot parameters 59
Table 9 File management commands 60
Table 10 History commands 63
Table 11 TOS values 183
Table 12 RIP supply and listen settings and switch action 214
Table 13 Monitor and show commands 305
Table 14 CLI command list 309
Table 15 Last byte of physical MAC address 346

Preface

The Nortel Networks™ Passport® command line interface (CLI) is used to configure and manage a Passport 1000 Series switch. The CLI, as well as the Passport Management Software graphical user interface (GUI), allows you to set up, configure, and manage your Passport switch as a layer 2 (switching) or layer 3 (routing) device.

This guide provides information about using the features and capabilities of the CLI to perform network management operations on Passport switches. It also contains a complete list of CLI commands. For general information about networking features in Passport products, refer to *Networking Concepts for the Passport 1000 Series Switch*. For information about using the Passport Management Software Device Manager, refer to *Reference for Passport Management Software Switching Operations*, and *Reference for Passport Management Software Routing Operations*.

Before you begin

Caution: Nortel Networks does not recommend or support IP Multicast with IGMP or DVMRP on the Passport 1000 platform.

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12`
`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is `ethernet/2/1 [<parameter> <value>]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is `show at <valid_route>`, *`valid_route`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP command on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Related publications

For more information about using a Passport 1000 Series switch or other Passport switches, refer to the following publications:

- *Networking Concepts for the Passport 1000 Series Switch* (part number 205588-B)

  Contains general information and descriptions about how the Passport switch handles various networking features, such as VLANs, MultiLink Trunking, OSPF, RIP, IPX, and so forth.

- *Reference for Passport Management Software Switching Operations* (part number 205586-B)

  Describes how to use Device Manager to configure and manage layer 2 (switching) functions with the Passport switch, including procedures and illustrations of pertinent screens.

- *Reference for Passport Management Software Routing Operations* (part number 205587-B)

  Describes how to use Device Manager to configure and manage layer 3 (routing) functions with the Passport switch, including procedures and illustrations of pertinent screens.

- *Installing the Passport 1000 Series Chassis* (part number 893-01051-E)

  Outlines the procedures for installing and booting your Passport switch and basic switch configuration, as well as instructions for installing the Passport Management Software.

- *Release Notes for the Passport 1000 Series Products Software Release 2.1* (Nortel Networks part number 896-00181-F)

  Describes important information about the software and hardware that is not covered in other related publications.

For more information about networking concepts, protocols, and topologies, consult the following sources:

- RFC1058 (RIP version 1)
- RFC 1723 (RIP version 2)
- RFC 1213 (IP)
- RFC 1389 (RIP 2 Management Information Base)
- RFC 1493 (Bridge MIB)
- RFC 1573 (IANAIf Type)
- RFC 1643 (Ether-like MIB)
- RFC 1757 (RMON)
- RFC 1850 (OSPF MIB)
- RFC 1583 (OSPF)
- RFC 2178 (OSPF)
- RFC 2338 (VRRP)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- Enterprise MIB (located on the *Passport 1000 Series Software CD*)

Hard-copy technical manuals

You can print selected technical manuals and release notes, directly from the Internet using the following URL www25.nortelnetworks.com/library/tpubs/. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Use the following Adobe Systems URL to download a free copy of the Adobe Acrobat Reader www.adobe.com URL to

You can purchase selected documentation sets, CDs, and technical publications through the Internet using the following URL www1.fatbrain.com/documentation/nortel/ URL.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
Passport basics

The Nortel Networks Passport 1000 Series of switches provides high-speed packet forwarding combined with the control of Internet Protocol (IP) routing. Passport switches support Gigabit Ethernet technology as well as conventional 10 megabits per second (Mb/s) and 100 Mb/s environments, combining layer 2 switching with layer 3 routing. For information about features supported in Passport switches, refer to *Networking Concepts for the Passport 1000 Series Switch*.

The Passport 1000 Series includes the following models:

- The Passport 1100 Switch
- The Passport 1150 Switch
- The Passport 1200 Switch

You can manage these switches using the Device Manager graphical user interface (GUI) or the command line interface (CLI).

Note: For procedures to perform initial setup of the switch configured for basic switching and routing operation, refer to *Installing the Passport 1000 Series Chassis* shipped in hard copy and on the Passport Documentation CD.

This chapter provides information about the basic operation of a Passport 1000 Series switch. Topics covered in this chapter include the following:

- "Management tools," next
- "Boot sequence" on page 36
- "Flash/PCMCIA file system" on page 40
- "Passport access levels and passwords" on page 52

Management tools

You can monitor and manage your Passport switch using the following tools:

- Device Manager
- Boot Monitor command line interface
- Run-Time command line interface
- Passport Configuration Page

Device Manager

Device Manager is an SNMP-based graphical user interface tool designed to manage single devices. In order to use this tool, you must have network connectivity to a management station running Device Manager on one of the supported platforms. Device Manager is the most versatile management tool in the Passport 1000 Series switch suite. It provides all the functionality you need to manage a single device, including the ability to create policy-based virtual LANs (VLANs).

For more information about using Device Manager, refer to *Reference for Passport Management Software Switching Operations* and *Reference for Passport Management Software Routing Operations*.

Boot Monitor command line interface

The Boot Monitor command line interface (CLI) contains commands that enable you to configure boot options and manage files in flash memory. Changes that you create and save within the Boot Monitor CLI are boot choices, flags, IP configuration, and Trivial File Transfer Protocol (TFTP) information. For the Boot Monitor command list, enter `help` at the monitor prompt. For more information about the Boot Monitor CLI, refer to Chapter 2, "Boot Monitor command line interface."

Run-Time command line interface

The Run-Time CLI performs most Passport management tasks. To access the Run-Time CLI, you need a direct connection to the switch from a terminal or PC. Use a null-modem cable to connect the console port (DTE DB-9 male interface) to a DTE terminal or PC. Communication parameters are as follows:

- 9600 bits per second (bps)
- 8 data bits
- No parity
- One stop bit
- Hardware flow control

For pinout information about required cables, refer to Appendix A in *Using the Passport 1000 Series Switch.*

You can also access the Run-Time CLI through a Telnet or rlogin session.

Many Run-Time CLI commands are listed and defined in this manual.

Passport Configuration Page

The Passport Configuration Page is a Web-based graphical user interface tool that operates with a Web browser. It has limited functionality and is intended for use as a tool to access and monitor devices on your network from various locations. For more information about using the Passport Configuration Page, refer to the section about "Web Management" in *Reference for Passport Management Software Switching Operations.*

Boot sequence

Passport 1000 Series switches go through a four-stage boot sequence.

The boot sequence includes the following four stages:

- Stage 1: Boot monitor image load
- Stage 2: Boot configuration load
- Stage 3: Run-time image load
- Stage 4: Switch configuration load

The following sections describe the stages in the boot process.

Stage 1: Boot monitor image load

When you power up or reset a switch, the processor on the Silicon Switch Fabric (SSF) module or board loads the boot monitor image. The boot monitor image is contained in flash memory on the SSF module. If a Passport 1200 Switch contains a redundant SSF module, one SSF module becomes the master SSF module when powering up or resetting. The boot monitor image is loaded from the flash memory on that SSF module.

When the boot monitor image is loaded, the CPU and basic system devices such as the console port, modem port, PCMCIA card slot (if applicable), and debug Ethernet port are initialized.

Note: I/O ports are not available at the boot monitor image load stage. The I/O ports are not initialized until later in the boot process.

Stage 2: Boot configuration load

After the bootstrap image loads, the boot configuration is loaded. The boot configuration resides in boot flash memory on the SSF module. It consists of parameters that control how the boot process proceeds and how the devices initialized by the boot monitor are configured. For information about boot monitor commands, refer to Chapter 2, “Boot Monitor command line interface”.

Table 1 lists the boot monitor parameters.

Table 1 Boot monitor parameters

Parameter	Description
Autoboot	Switch automatically proceeds to stage 3. If you do not want autoboot to proceed, you can interrupt the sequence at stage 2 using the console port.
Factory Configuration	Determines whether the factory default configuration or a user-defined configuration is used. For more information, refer to "Stage 4: Switch configuration load."
Isolate All I/O Ports	Disables all bridging and routing and isolates all I/O ports.
Run-time Image Sources	Specifies up to three run-time image sources and the order in which they are loaded. For more information about this process, refer to "Stage 3: Run-time image load."
Config File	Allows you to specify which configuration file to use as the boot source: flash, PCMCIA, or a script file. If not specified, the boot file is used.
IP Address	Provides the IP address for the diagnostic Ethernet port.
TFTP Server	A default TFTP server and file to retrieve for the bootstrap TFTP client.

If Autoboot is disabled or interrupted at the console, the boot process stops. At this stage, the user has access to the Boot Monitor CLI at the console.

You can set the boot configuration and perform upgrades to the bootstrap image and run-time image (loaded in stage 3) in the Boot Monitor CLI. Any changes made and saved at the Boot Monitor CLI change the boot configuration.

After you save the configuration, you can reinitiate the boot process from the Boot Monitor CLI using the `boot` command.

Stage 3: Run-time image load

The run-time image loads after the boot configuration. This software image initializes the I/O modules and provides full switch functionality.

You can load the run-time image from various sources depending on the model of the Passport switch:

- Passport 1200 switches can load the run-time image from the flash memory, from a PCMCIA card, or from a TFTP server using the diagnostic Ethernet port.
- Passport 1100/1150 switches can load the run-time image from the flash memory or from a TFTP server using the diagnostic Ethernet port.

The factory default load order is as follows:

- PCMCIA (if applicable)
- Flash memory
- TFTP (if applicable)

However, you can define the source and order from which to load the run-time image:

- To specify the order in the Boot Monitor CLI, enter the **`choices`** command. See "Boot commands" on page 59.
- To specify the source using the Run-Time CLI commands, enter the **`config sys set boot`** command. See the description on page 117.

Stage 4: Switch configuration load

Before continuing to the boot process, load the switch configuration. The switch configuration includes:

- Chassis configuration
- Port configuration
- Spanning tree group configuration
- VLAN configuration
- Routing configuration
- IP address assignments
- RMON configuration

The default configuration includes:

- A single, port-based default VLAN with a VLAN identification number of 1, bound to the default spanning tree group.
- All ports in a single spanning tree group, STG number 1. (The default spanning tree group is 802.1D compliant, and its BPDUs are never tagged.)
- Spanning Tree FastStart disabled on all ports.
- No interfaces assigned IP addresses.
- Traffic priority for all ports set to normal priority.
- All ports as nontagged ports.

The boot configuration determines whether a switch configuration is loaded, and you can bypass loading the switch configuration.

To bypass loading the switch configuration in the Boot Monitor CLI:

1. Enter the **`flags`** command. You are prompted:

   ```
   Do you want to use the factory default configuration (y/n)?
   ```

2. Enter `y`.

To bypass loading the switch configuration in the Run-Time CLI:

➔ Enter the **`config sys set flags factory default true`** command.

When you bypass the configuration, the switch boots using the factory default configuration, except the boot configuration settings are loaded in stage 2. Bypassing the switch configuration does not affect the saved switch configuration; the configuration is not loaded.

Flash/PCMCIA file system

This section describes the flash/PCMCIA file system in a Passport switch running release 2.X software. The flash file system in a Passport 1000 Series switch holds executable images and switch configuration. The following sections are included:

- "Flash memory organization," next
- "File types" on page 41
- "Devices and file names" on page 43
- "File system commands" on page 45

Flash memory organization

The Passport switch has two onboard flash memory devices: Boot Flash and System Flash. A Passport 1200 Series switch can use optional PCMCIA flash cards (refer to "PCMCIA (pcmcia:)" on page 41).

Boot Flash

The Boot Flash memory is 512 kilobytes (KB) and is divided into the following reserved areas for the boot monitor image and the switch configuration:

- Boot monitor image

  The boot monitor image is not directly user accessible. It is updated using a special boot monitor updater that writes to the area reserved for the boot image.

- Switch configuration (config and nvram)

  The switch configuration is written whenever a save operation is performed on the configuration of the device. By default, the switch configuration is stored in a reserved area in Boot Flash, although it is possible to specify alternative locations in the file system for the switch configuration.

  — In the Boot Monitor CLI, enter the **`choice`** command.

  — In the Run-Time CLI, enter the **`config sys set config <choice>`** command.

The area reserved in Boot Flash for switch configuration is accessed by the file system commands using the config or nvram file names. Both config and nvram refer to the same file. Note that the switch configuration is read only when the run-time image loads.

System Flash (flash:)

The System Flash memory is 4 megabytes (MB) and is primarily used for run-time images, the system log, configuration files, and other general storage. It is divided into 64K blocks. Files stored in System Flash are stored in an integral number of blocks.

Files stored in System Flash are numbered sequentially starting with number one. Files are assigned names by the user or referenced by an ordinal position in flash memory. The file naming convention for System Flash files is "flash:*filename*" or "flash:*file#*." For example, flash:3 and flash:acc2_0_0 both refer to files in System Flash. In the first example, it is the third file in System Flash. In the second example, it is the file named acc_2_0_0 in System Flash.

PCMCIA (pcmcia:)

A Passport 1200 Switch can use an optional PCMCIA flash memory card. You can use PCMCIA cards for general storage of all file types.

The PCMCIA card used in the Passport 1200 Switch is the XLR1299PC PCMCIA Flash Memory Module. It has a capacity of 4 MB of memory with a block size of 128K. As with System Flash, files stored on PCMCIA are numbered sequentially starting with number 1 and can be given file names. Use the following naming convention for PCMCIA files: "pcmcia:*filename*" or "pcmcia:*file#*."

File types

Although System Flash and PCMCIA are primarily used for run-time images, configuration files, and the system log, they are also used to store other types of files. The following sections describe the types of files you can store in the System Flash and PCMCIA. For a given file, the file type is reflected in the flags in a directory listing (see "Directory" on page 46).

Executables

Executables are images that are executed by the Passport 1000 Series Central Processing Unit (CPU). The two most common executables are run-time images and boot monitor updaters. Executables are stored in the flash file system in zipped (compressed) format. The switch automatically unzips (uncompresses) the file on execution.

- Run-time images

  The run-time image is an executable file that executes after the boot monitor image, initializing the I/O modules and providing full switch functionality. You can store and execute run-time images from System Flash and PCMCIA.

- Boot monitor updaters

  The boot monitor image is low-level code that initializes devices on the SSF module and starts the boot process. The boot monitor image is updated by executing a boot monitor updater that replaces the image stored in Boot Flash.

Log files

Console information, warning, and error messages are logged to a log file. The log file is stored in System Flash. On a Passport 1200 Switch, if insufficient space is found at initialization, the log is created in the PCMCIA. If no log file is present when the run-time image executes, a new log file is created. Log files are 128K, divided into two 64K banks. When the second bank fills, the first bank is erased and used again.

Configuration files

In addition to the area reserved in Boot Flash for the switch configuration, you can store and use configuration files in System Flash and PCMCIA.

Script files

Script files are ASCII-based text files containing CLI commands that are read by the switch. The commands are executed as though they are typed during a console session.

Trace logs

For debugging purposes, the switch creates a trace log with diagnostic messages. The trace log is not normally activated, so it is not normally accessed by users. The file system commands refer to the reserved “trace” area for the trace log.

Devices and file names

The Passport 1000 Series Switch (I/C) file system supports file naming and a device file number referencing scheme. There are also reserved device names for reserved areas in flash memory.

System Flash and PCMCIA file names

System Flash and PCMCIA support file names. A file name can be up to 31 characters and can include printable characters and spaces. File names must begin with a nonnumeric character. The file name format is where:

device is the file name.

device indicates whether the file resides on flash or PCMCIA.

filename is the name of the file.

If the file name includes spaces, enclose the entire file name in quotes when used as an argument for a command. For example, entering the command:

```
copy flash:acc2_x_x “pcmcia:old image file”
```

copies the **acc2_x_x** in System Flash to the file “old image file” on PCMCIA.

Duplicate file names are allowed on a device. The file name with the highest file number (the last, nondeleted file) is the active command file.

You can also reference a file on System Flash and PCMCIA according to the device on which it resides and its ordinal position on the device by entering the command:

```
<device>:<file#>
```

where:

device indicates whether the file resides on flash or PCMCIA.

file# is the file number on the device.

For example, the first file on System Flash is flash:1, and the second file on PCMCIA is pcmcia:2. You can abbreviate device names to two letters. For example, flash:2 and fl:2 refer to the same file.

Reserved devices

The file system commands use device names or file names as arguments. Reserved device names have special meaning when used as command arguments. Table 2 describes the reserved command arguments and their meanings.

Table 2 Command arguments and meaning

Command Arguments	Meaning
Config and nvram	The config and nvram device names refer to the area of Boot Flash reserved for the switch configuration. You can copy files to and from the config and nvram areas.
TFTP	Use the tftp device name to copy files to and from a Trivial File Transfer Protocol (TFTP) server. When the TFTP device is used as a source or destination, you are prompted for the IP address of the TFTP server and the remote file path. TFTP client is built into the switch that affects the file transfers with the TFTP server.

Table 2 Command arguments and meaning (continued)

Command Arguments	Meaning
Trace	The trace device name refers to a reserved area of system RAM where the switch writes debugging messages. The trace log is not normally activated, so it is not normally accessed by users. The file system commands refer to the reserved trace area for the trace log.
Running config	The running config is the configuration currently running on the SSF module. The name is only used as a parameter for the **copy** command (see page 49). When used as the source of a copy, the destination requires a script file name for the current switch configuration. When used as the destination, the source must be a script file with CLI commands used to make incremental changes to the current configuration state.

File system commands

The flash file system commands allow all the basic operations of any file system. The commands use the format **command <arguments>**. Both the commands and the arguments can be abbreviated, as long as the abbreviation is not ambiguous. Table 3 lists the Passport file system commands.

Table 3 Passport file system commands

Command	Abbreviation	Description
format	fo	Formats flash or PCMCIA.
directory	di	Lists contents of flash or PCMCIA.
copy	co	Copies a file to a device appending a new file to the destination device.
delete	de	Marks a file for deletion on a flash device.
squeeze	sq	Reclaims space used and removes files marked for deletion.
recover	re	Unmarks a file for deletion.

Format

The **format** command permanently erases a device, preparing the device for use. To permanently erase a device, enter the command:

```
usage: format <device>
```

where:

device indicates whether the file resides on flash or PCMCIA.

It is advisable to run the **format** command on any new PCMCIA card to ensure that it is ready for use by the Passport 1000 Series file system.

Directory

The **directory** command displays the contents of flash or PCMCIA. To display the contents of flash or PCMCIA, enter the command:

```
usage: directory [<device>][-l]
```

where:

device indicates whether the file resides on flash or PCMCIA.

-l displays the file details.

When the **directory** command is invoked with no arguments, it displays the contents of all flash devices. When a device is specified, **directory** displays only the contents of that device. Information included in the directory output includes the file number (FN), file name (Name), file size (Length), and file flags (Flags). Flags display information about the file type and whether it is compressed or marked for deletion. Table 4 lists the directory flags.

Table 4 Passport directory flags

Flag	Description
C	Configuration file
X	Executable file
Z	Compressed file (gzip format)

Table 4 Passport directory flags (continued)

Flag	Description
D	Marked for deletion
L	Log file
N	Directory entry in named format
T	Trace file
S	Script file - an ASCII configuration file

In Figure 1, files 1 is a log file, file 2 is a script file, file 3 is a configuration file, file 4 is a compressed executable file, and file 5 is a configuration file.

Figure 1 Passport 1200 directory flash command example

```
swlab-edge2# directory flash
Device: flash
FN Name                              Flags    Length
-- ----                              -----    ------
1  syslog                              LN    131072
2  dana.cfg                            SN     14161
3  dana.cfg                            CN     12788
4  p10a2100.img                       XZN   2061580
5  config.cfg                          CN     12888
--                                            ------
5   files                      bytes used=   2424832 free=1769472
```

The `-l` option in the **`directory`** command shows the file details. In particular, it shows the original file name of run-time executables.

There are no file compression commands in the CLI. A zipped executable file that is copied to the file system is automatically unzipped on execution.

The sample output of the **`directory flash`** command in Figure 2 shows that three images currently reside in flash memory.

Figure 2 Passport 1100 directory flash command example

```
Passport 1100# directory flash
Device: flash
FN Name                              Flags    Length
-- ----                              -----    ------
1  syslog                              LN    131072
2  p10a2100.img                       XZN   2061580
3  config.cfg                          CN     18188
--                                             ------
3   files                      bytes used=  2293760 free=1900544
```

Copy

The **copy** command copies an image from a source device to a destination device. To copy an image from a source device to a destination device, enter the command:

usage: copy <*srcdevfile*> <*destdevfile*>

where:

srcdevfile is the file name or number of the source file in flash, PCMCIA, config, nvram, tftp, or trace.

destdevfile is the file name or number of the destination file in flash, PCMCIA, config, nvram, or tftp.

For the **copy** command, the source is a specific file or a reserved device name.

If a destination file name is not specified, the file name remains the same as the source file name. The **copy** command appends the file to the last unused memory block on the device.

Using the **copy** command, a run-time image is copied to flash from a TFTP server. The source argument is tftp, not a file name. The system prompts the user for the TFTP server IP address and the remote file path (Figure 3).

Figure 3 copy command

```
Accelar-1200# copy tftp flash
Enter source tftp server address [10.125.2.205]:
Enter source file [cfg]: cfg
tftp result: success
Accelar-1200# dir
```

The system appends the file to the last unused block of memory on flash, so there are three files in flash (Figure 4).

Figure 4 directory flash command

```
Passport 1100# dir
Device: flash
FN Name                              Flags    Length
-- ----                              -----    ------
1  syslog                              LN    131072
2  p10a2100.img                       XZN   2061580
3  config.cfg                          CN     18188
--                                             ------
3   files                     bytes used=   2293760 free=1900544
```

Copy script file to running config

An extension of the **copy** command allows a script file (an ASCII-based text file containing CLI commands) to be read by the switch. The commands are executed as though they were typed during a console session. By default, script execution does not display at the device where the command is issued. However, if the optional debug parameter is used, the execution of the command in the script file and the results are output to the device from which the command was executed.

The script file is an ASCII text file. The first line of the file must include a pound sign (#) followed by a carriage return, with the remaining lines containing one valid CLI command per line.

To use a script file for switch configuration, enter the command:

`copy <sourcedevice:filename> running-config [debug]`

where:

`sourcedevice:` is a flash, PCMCIA, or TFTP-based file server. If “tftp” is specified, you are prompted for the server IP address and file name.

`filename` is the name of the file to be copied.

`[debug]` is the optional parameter that allows you to view the script while it is executing.

Note: Use caution when executing script files from within the CLI. The command executes references from your current position in the directory structure.

Delete

The **`delete`** command marks a file for deletion on a device: To mark a file for deletion, enter the command:

`usage: delete <devfile>`

where:

`devfile` is the file name or number of the flash or PCMCIA file and the device name or number you can include.

Note: The **`delete`** command marks a file for deletion, it does not erase the file. To free the space used by a deleted file, use the **`squeeze`** command.

Squeeze

The **squeeze** command reclaims deleted file space on a device. To reclaim deleted file space, enter the command:

```
usage: squeeze <device>
```

where:

device is flash or PCMCIA. You can also include a device name or number.

Note: The files are renumbered after using the **squeeze** command.

Recover

The **recover** command is used to unmark all files on the device already marked for deletion. To recover marked files before a delete, enter the command:

```
usage: recover <device>
```

where:

device is flash or PCMCIA.

Passport access levels and passwords

The Passport 1000 Series switch has six levels of security access for device management. Table 5 describes the access levels and lists their default login names and passwords.

Table 5 Access levels and default login names and passwords

Access level	Description	Default login	Default password
Read-only	Allows only viewing of configuration and status information and is equivalent to SNMP read-only community access.	ro	ro
Layer 1 (read/write)	Allows viewing and changing configuration and status information for layer 1 (physical layer) functions.	l1	l1
Layer 2 (read/write)	Allows viewing and changing configuration and status information for layer 1 and layer 2 (bridging/switching) functions.	l2	l2
Layer 3 (read/write)	Allows viewing and changing configuration and status information for layer 2 and layer 3 (routing) functions.	l3	l3
Read/write	Allows viewing and changing configuration and status information across the switch. It does not allow changing security and password settings and is equivalent to SNMP read/write community access.	rw	rw
Read/write/all	Allows all the rights of Read-Write access *and* the ability to change security settings, including the CLI and Web-based management user names and passwords and the SNMP community strings.	rwa	rwa

For example, if you want to log on with read/write/all access through the console port, log on as rwa using the password rwa at the login prompt.

Telnet and console passwords

When a Passport 1000 Series Switch is accessed for management, the user is prompted for a login name and password. Table 6 lists the default login and password values for console and Telnet sessions.

Table 6 Login and password default values

Access level	Default login	Default password
Read-only	ro	ro
Layer 1 read/write	l1	l1
Layer 2 read/write	l2	l2
Layer 3 (and layer 2) read/write	l3	l3
Read/write	rw	rw
Read/write/all	rwa	rwa

You can change logins and passwords only if you log in with Read-Write-All privileges (rwa access level). You can also change the login name for different modes. When the CLI prompts for login and password, the access level is set according to the login and password entered.

The **`login`** command allows you to log in again using a different login access by entering the user name and password.

Note: The prompt remains at the same level that you were before logging in again.

The **`logout`** command allows you to log out and reenter at the top level prompt. If you connect to the switch through Telnet, the logout command terminates the Telnet session.

CLI commands to change the console/Telnet password

You can use the following commands to change the console/Telnet login name and password for each login access level:

- **`config cli password ro <username>[<password>]`**—changes the read-only login and/or password.
- **`config cli password l1 <username>[<password>]`**—changes the Layer 1 read/write login and/or password.
- **`config cli password l2 <username>[<password>]`**—changes the Layer 2 read/write login and/or password.
- **`config cli password l3 <username>[<password>]`**—changes the Layer 3 read/write login and/or password.
- **`config cli password rw <username>[<password>]`**—changes the read/write login and/or password.
- **`config cli password rwa <username>[<password>]`**—changes the read/write/all login and/or password.

where:

`username` is the login name.

`password` is the password associated with the login name.

Chapter 2
Boot Monitor command line interface

The Boot Monitor CLI commands enable you to configure boot options and manage files on the flash module. Boot monitor CLI commands are used when the switch is not active. These commands enable you to perform the following tasks:

- Configure and display boot options, including the configuration file
- Manage the NVRAM (flash) file system
- Configure and change IP parameters for system devices
- Change boot flags
- Reset or reboot the system with the default configuration
- Reset or reboot the system from a different boot source

This chapter describes the Boot Monitor CLI and covers the following topics:

- "System and station requirements," next
- "Accessing the Boot Monitor CLI" on page 56
- "Boot monitor command list" on page 56

System and station requirements

You can use any terminal or personal computer (PC) with a terminal emulator as the CLI command station. The terminal requires the following:

- 9600 bits per second (b/s), 8 data bits, 1 stop bit, no parity, no flow control
- Serial terminal-emulation program such as Terminal or Hyperterm for Windows NT® or Hyperterm for Windows® 95 or Windows 98
- Cable and connector to match the Passport switch male DTE connector (DB-9)

Accessing the Boot Monitor CLI

To access the Boot Monitor CLI, do one of the following:

- Interrupt the boot sequence by pressing a key at the following prompt:

  ```
  Press any key to stop autoboot
  ```

  or
- From the run-time CLI, enter the following commands:

  ```
  config sys set flags autoboot false
  save
  ```

Then reboot the system.

When you enter the Boot Monitor CLI, the following prompt displays:

```
monitor>
```

Boot monitor command list

For a boot monitor command list, at the monitor prompt, enter:

```
help commands
```

For information about the boot load process, see “Boot sequence” on page 36.

Table 7 lists the Boot Monitor CLI commands and the reference page numbers for more information.

Table 7 Boot Monitor CLI commands

Command	See page
Boot commands—Use these commands to display and modify boot parameters and to reboot the Passport 1000 Series chassis. **boot [device> [:filename] <*cfgfile*> [<*tftp*> <*file*>]]** **choices [<choice> <*source*>[:<*filename*>]]** **devices [<*device name or device number*>]** **flags** **reset [-y]** **save** **tests [<*device name or device number*>]** **tftp [<*server ip address*> <*file*>]** **Note:** Entering a boot command with no arguments causes the switch to follow the current boot choices and boot the switch.	59
File and device management commands—Use these commands to manage system software files and configuration files and to manage the flash module and PCMCIA card. **copy [<*src device*>[:filename] <*dest device*> [:filename>]]** **delete <*device name or device number*> <:*filename*>** **directory <*device name or device number*>** **format <*device name or device number*>** **recover <*device name or device number*>** **squeeze <*device name or device number*>**	60
`help` command—Use this command to list all boot monitor commands or to display command syntax. **help <*command*>**	62

Table 7 Boot Monitor CLI commands (continued)

Command	See page
history commands—Use these commands to display and reenter commands. Syntax is the same as the run-time CLI history command. **!!** **!<*number*>** **!<*str*>** **!?<*substr*>** **^<*sstr*>^<*rstr*>**	62
ip command—Use this command to assign an IP address to the diagnostic Ethernet port. **ip [<*device*> <*ipaddr*> <*netmask*> <*gateway*> <*mgmtnet*>]**	63
ping command—Use this command to test the network connection between the Passport 1000 Series chassis diagnostic port and another networking device. **ping <*device*> <*ipaddr*> [<*size*>]**	65
quit command—Use this command to end the Boot Monitor CLI session and reboot the Passport 1000 Series chassis. **quit**	67
show command—Use this command to display boot configuration parameters. **show [<*configuration type*>]**	65
log command—Use this command to display system log information. **log create<*device*>** **log clear <*device*>: <*filename*> <*nblocks*>** **log show <*device*> <*filename*> [tail]**	60
trace command—Use this command to display trace file information. **trace show [tail] <*device*> [*:filename*>]**	60

Boot commands

A **boot** command enables you to display and modify a boot parameter and to reset or reboot the system.

Note: Entering a **boot** command with no arguments causes the switch to follow the current boot choices and boot the switch.

Table 8 lists the Boot Monitor CLI boot parameters.

Table 8 Boot Monitor CLI boot parameters

Command	Description
boot [<*device*> [:filename] <*cfgfile*> [<*tftp*> <*file*>]]	Boots the switch. • *device* is the name or number of a boot device. • filename is the software image file name. • *cfgfile* is the software configuration device and file or NVRAM file name. • *tftp file* specifies a file that is on the TFTP server.
choices [<*choice*> <*source*> [:<*filename*>]]	Displays or changes the order in which the boot sources (flash and PCMCIA card) are accessed. • *choice* is the order in which the specified boot device is accessed when you reboot the switch: primary, secondary, or tertiary. • *source* is the boot source (none, flash, pcmcia, net, skip). If you specify none, no boot source is accessed for the choice (primary, secondary, or tertiary) you are configuring. If you specify skip, the choice you are configuring is skipped.
devices <*device name or device number*>	Enables or disables the specified boot device.
flags	Enables or disables autoboot and booting using the default configuration settings.
reset [-y]	Resets the system by loading the configuration file or by using the default settings.
save	Saves changes to the boot configuration parameters.
show	Displays the boot configuration parameters.
tests <*device name or device number*>	Enables or disables the bootup diagnostic tests.

Table 8 Boot Monitor CLI boot parameters (continued)

Command	Description
tftp	Changes TFTP server information.
help	Lists all boot monitor commands or displays a command syntax.

To list the boot devices on your routing switch, enter the **show devices** command.

To list the file names, enter the **directory** command.

The **flags**, **reset**, **save,** and **tftp** commands do not require parameters; **flags** and **tftp** commands prompt you to select options.

File and device management commands

The file and device management commands enable you to manage files on the boot devices (flash, PCMCIA card, and TFTP server). In addition, these commands allow you to manage the flash module and PCMCIA card.

The file management commands include those listed in Table 9.

Table 9 File management commands

copy <*src device*> [:filename] <*dest device*> [:filename] where: *src device* is the device from which you are copying a file. *dest device* is the device onto which you are copying a file. *filename* is a file name.	Copies a file from one boot device to another, or copies it to the same boot device using a new file name. With no arguments, it prompts the user.
delete <*device*> [*:filename*>	Deletes a file from a flash or PCMCIA device.

Table 9 File management commands (continued)

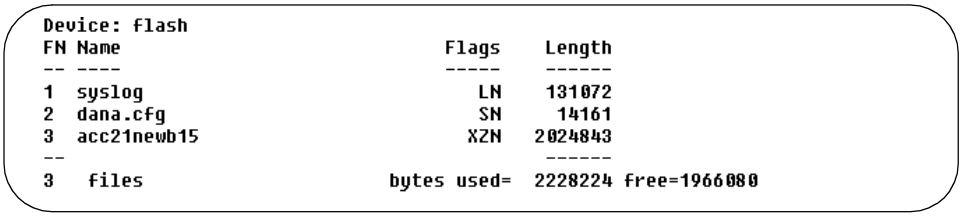
directory <*device name or device number*> [-l] where: *device name or device number* is the file device: flash or PCMCIA. [-l] represents file details.	Lists the files on a flash or PCMCIA device.
format <*device name or device number*>	Formats the flash module or PCMCIA card.
recover <*device name or device number*>	Recovers a file deleted from the flash module or PCMCIA card.
squeeze <*device name or device number*>	Reclaims space occupied by files marked for deletion on the flash module or PCMCIA card.
log show <*device*> <*:filename*> [tail]	Displays system log information. **Note:** [tail] requests displaying information from the back first.
log create <*device*> [:<*filename*>] <*nblocks*>	Creates a log file. **Note:** [nblocks] is the number of blocks to be displayed.
log clear <*device*> [:*filename*>	Clears log files on a device or the specified log file.
trace show [tail] <*device*> [:*filename*>]	Displays trace information. **Note:** [tail] requests displaying information from the back first.

To list devices on your Passport 1000 Series chassis, use the **show devices** command.

To list the file names, enter the **directory** command.

Figure 5 shows output for the **directory** command.

Figure 5 directory command output



```
Device: flash
FN Name                                Flags    Length
-- ----                                -----    ------
1  syslog                                LN    131072
2  dana.cfg                              SN     14161
3  acc21newb15                          XZN   2024843
--                                              ------
3   files                      bytes used=  2228224 free=1966080
```

Help commands

Help is available at all levels of the CLI by typing `?` or `help`. Typing `help` displays a list of the boot monitor commands.

History commands

The **`history`** commands list the commands you have entered during the current session and allow you to reenter commands.

Table 10 describes the history commands.

Table 10 History commands

Command	Description
history	Lists the commands that you have entered during the current CLI session.
!!	Reenters the most recently entered command.
!<*number*>: run command <*number*>	Enters the command identified in the command history by *<number>*.
!<*str*>	Runs the last command that matches the given string *<str>*.
!?<*substr*>	Runs the last command that matches the given substring *<substr>*.
^<*sstr*>^<*rstr*>	Enters the most recent command but substitutes a new string for a given string.

IP command

The **ip** command assigns an IP address to the diagnostic Ethernet port for troubleshooting and diagnostics.

Note: For normal operation, do not have an IP address assigned to the diagnostic Ethernet or serial port. Set the IP address to 0.0.0.0.

The syntax for the **ip** command is:

ip [<*device*> <*ipaddr*> <*netmask*> <*gateway*> <*mgmtnet*>]

where:

ipaddr is the IP address in dot notation.

ipaddr is the network device name or number.

netmask is the subnet mask.

gateway is the default router IP address.

mgmtnet is the management station network IP address. Use this argument only if the management station is on a different subnet. If you use this argument, the Passport 1000 Series chassis enters a static route to the management network in the routing table.

If you do not use any of the arguments, the CLI prompts you for information.

Figure 6 shows an example of the **ip** command. In this example, the command is issued without arguments, so the CLI prompts for the argument values.

Figure 6 ip command output

```
monitor> ip
---   CHANGE IP ADDRESS   ---
 Net Devices:
-----------------------------------------------------------------
 4    Enabled     Serial Port 2 [s2] hw=ff:ff:ff:ff:ff:ff
                  ip=0.0.0.0 netmask=0x00000000
                  mgmt net=0.0.0.0 gateway=0.0.0.0
 5    Enabled     Debug Ethernet [nic] hw=00:e0:16:04:66:00
                  ip=0.0.0.0 netmask=0x00000000
                  mgmt net=0.0.0.0 gateway=0.0.0.0
-----------------------------------------------------------------
select network interface device [5]:
Enter ip address [0.0.0.0]:
Enter netmask [255.0.0.0]:
Enter default gateway [0.0.0.0]:
Enter Mgmt Network [0.0.0.0]:
 Net Devices:
-----------------------------------------------------------------
 4    Enabled     Serial Port 2 [s2] hw=ff:ff:ff:ff:ff:ff
                  ip=0.0.0.0 netmask=0x00000000
                  mgmt net=0.0.0.0 gateway=0.0.0.0
 5    Enabled     Debug Ethernet [nic] hw=00:e0:16:04:66:00
                  ip=0.0.0.0 netmask=0xff000000
                  mgmt net=0.0.0.0 gateway=0.0.0.0
-----------------------------------------------------------------
ip configuration has been saved
```

Note: The Net 4 Serial port entry applies only to the modem port on the Passport 1200 Switch. You cannot assign an IP address to this port in software release 2.1.

Ping command

The boot monitor **ping** command allows you to test the connection between the Passport 1000 Series chassis and another networking device.

The syntax for the boot monitor **ping** command is:

ping <*ipaddr*> [<*datasize*> <*count*>]

where:

ipaddr is the IP address of the other networking device.

datasize count is any integer value equal to or greater than 1. The default is 1.

Figure 7 shows an example of ping output.

Figure 7 ping command output

```
monitor> ping
---   PING TEST   ---
 Net Devices:
-----------------------------------------------------------------
 4    Enabled    Serial Port 2 [s2] hw=ff:ff:ff:ff:ff:ff
                 ip=0.0.0.0 netmask=0x00000000
                 mgmt net=0.0.0.0 gateway=0.0.0.0
 5    Enabled    Debug Ethernet [nic] hw=00:e0:16:04:66:00
                 ip=0.0.0.0 netmask=0xff000000
                 mgmt net=0.0.0.0 gateway=0.0.0.0
-----------------------------------------------------------------
select network interface device [5]:
Enter destination ip address [192.168.1.1]:
Enter ping size [48]:
Using [nic] to ping. press any key to stop.
ENET: hold frame collision, outbound frame.
2 packets transmitted, 0 packets received, 100% packet loss
monitor> ping
---   PING TEST   ---
 Net Devices:
-----------------------------------------------------------------
 4    Enabled    Serial Port 2 [s2] hw=ff:ff:ff:ff:ff:ff
                 ip=0.0.0.0 netmask=0x00000000
                 mgmt net=0.0.0.0 gateway=0.0.0.0
 5    Enabled    Debug Ethernet [nic] hw=00:e0:16:04:66:00
                 ip=0.0.0.0 netmask=0xff000000
                 mgmt net=0.0.0.0 gateway=0.0.0.0
-----------------------------------------------------------------
select network interface device [5]:
Enter destination ip address [192.168.1.1]:
Enter ping size [48]:
Using [nic] to ping. press any key to stop.
ENET: hold frame collision, outbound frame.
ENET: hold frame collision, outbound frame.
2 packets transmitted, 0 packets received, 100% packet loss
```

Show command

Note: The Net 4 Serial port entry applies only to the modem port on the Passport 1200 Switch. You cannot assign an IP address to this port in software release 2.1.

The **show** command displays chassis configuration information. The syntax for the show command is:

show [<*configuration type*>]

where:

configuration type is one of the following:

- info displays general chassis configuration information.
- ip displays IP configuration information.
- boot displays the boot choices.
- tftp displays information about the TFTP server.
- tests displays test information.
- devices displays information about the boot devices.
- environment displays information about the SSF module and chassis.

If you do not specify a configuration type, the CLI displays all the configuration information.

Quit command

The **quit** command ends your Boot Monitor CLI session and reboots the Passport 1000 Series chassis.

Chapter 3
Run-Time CLI description

In a Passport 1000 Series switch, the Run-Time CLI commands enable you to display and modify the switch configuration while the switch is operating. This chapter includes information about the Run-Time CLI in the Passport software. It includes the following sections:

- "System and station requirements," next
- "General usage" on page 70
- "Run-time command list tree" on page 76
- "Navigation commands" on page 78
- "General commands" on page 78
- "File and device management commands" on page 88
- "Test commands" on page 92
- "Trace commands" on page 94

System and station requirements

You can use any terminal or PC with a terminal emulator as the CLI command station. The terminal requires the following:

- 9600 bits per second (b/s), 8 data bits, 1 stop bit, no parity, no flow control
- Serial terminal-emulation program such as Terminal for Windows NT or Hyperterm for Windows 95 or Windows 98
- Cable and connector to match the Passport switch male DTE connector (DB-9)

You can access the CLI through a direct serial-port connection to the switch. For the Run-Time CLI, you can access the switch through a Telnet connection or asynchronous dial-up modem. Passport 1000 Series switches support up to two CLIs at the modem and console serial ports, and up to eight Telnet sessions.

Note: Some features require ARU2 or ARU3 hardware. To determine the hardware version in your chassis, use the **`show sys info`** command. The display indicates the ARU level of the chassis and, if applicable, the cards.

General usage

When the switch is up and running, the Run-Time CLI commands enable you to perform most of the configuration and management functions necessary to manage your Passport switch. These functions include the following:

- Resetting or rebooting the Passport 1000 Series chassis
- Saving your configuration to NVRAM (nonvolatile RAM)
- Adding, deleting, and displaying ARP table entries
- Configuring RIP, DHCP, OSPF, VRRP, IGMP, DVMRP, and IPX parameters
- Pinging another networking device
- Displaying and setting configuration parameters for the entire Passport 1000 Series chassis and for individual ports
- Adding and deleting static IP routes (including default routes) in the IP route table
- Configuring and displaying spanning tree group (STG) parameters and enabling or disabling Spanning Tree Protocol on an STG
- Configuring and displaying Multilink Trunking (MLT) parameters
- Setting IP policies for RIP and OSPF
- Setting traffic filters for the switch
- Testing the Passport 1000 Series chassis switching fabric and performing internal and external loopback tests on individual ports
- Creating and managing port-based VLANs or policy-based VLANs

Note: The CLI commands enable you to perform most configuration tasks. To perform a task not available using CLI commands, use the Passport Device Manager.

Passwords

There are six defined levels of password-protected access to the CLI:

- ro (read-only)
- L1 (layer 1 read/write)
- L2 (layer 1 and layer 2 read/write)
- L3 (layer 2 and layer 3 read/write)
- rw (read/write for all levels)
- rwa (read/write/all)

When you access the CLI, it prompts you for a login name and password, and sets your access level accordingly. Only users with rwa access can change login names and passwords.

Navigating through the CLI

The CLI is organized into a tree data structure. Help can be accessed from any level of the tree by typing a question mark (?). Typing the word "help" provides an explanation of the available help. Typing the **`help`** command explains what the command does and give the syntax. Typing `?` results in a list of all commands. Typing the word "syntax" displays a path list of commands and parameters available from the current prompt or `<command>` forward. It lists the syntax in the current context.

When you type a command, you may see context and subcontext. Context indicates commands at that level. Subcontext indicates one or more command layers available.

When you are within a given branch of the tree, you need to type only the subcommand for that level. For example, to enable IP forwarding (routing) from the top level, type: **`config ip forwarding enable`**. When you are already in the "config ip" branch, you need only type: **`forwarding enable`**.

After you have entered information to put you at a certain level, you remain at that level until you type **back** or reenter the original command. For example, when using the commands that begin with **config ethernet <*ports*> ip**, after you have entered a port number, you do not have to reenter this information unless you go back up a level. This feature enables you to create, delete, or change all relevant parameters for this port without reentering information.

To avoid having to type complete commands, you can enter a shortened version of the command, such as `dis` for disable or `en` for enable, or type part of a command and then press the Tab key to complete the command. If the letters you typed are unique to a command, the command is completed automatically. If not, a bell sounds to indicate that more information is necessary.

The following keystroke shortcuts are available in the CLI:

- Control-P—To view and scroll through the previous history commands.
- Control-N—To view and scroll through the next history commands.
- Control-U—To delete a line; clears the line and allows you to enter a new command.
- Control-C—To abort a line entry; aborts the command entry and puts you at a new prompt. Note that this command does not abort the current command level that is running, only the new entry.
- Control-D—To log off the system.
- Control-S/Control-Q—Software flow control XON/XOFF.
- Control-I—Command completion; completes the command when you have entered part of a word (sh for show).
- Control-H—Backspace.

In addition, certain commands are used for navigating through the CLI:

- **back**—takes you back one level.
- **box** or **top level**—takes you to the box or top level.
- **pwc**—displays the current working level.

Parameter values in the CLI are indicated by angle brackets (`< >`). Parameters are optional or required. Required parameters must be in the specified order, followed by optional parameters. Optional parameters are displayed in brackets ([ ]).

When entering multiple CLI commands, you can terminate a command within a single line of input by using the semicolon (;) as the separator. A semicolon is treated like a carriage return by the CLI.

Getting help

When navigating through the Run-Time CLI, you have online Help available at all levels. You can access Help at any time in the CLI by typing `?` or the word "help" anywhere in or on the command line. Refer to "Help command" on page 81 for more information about the specific types of online Help.

Port numbers and IP addresses

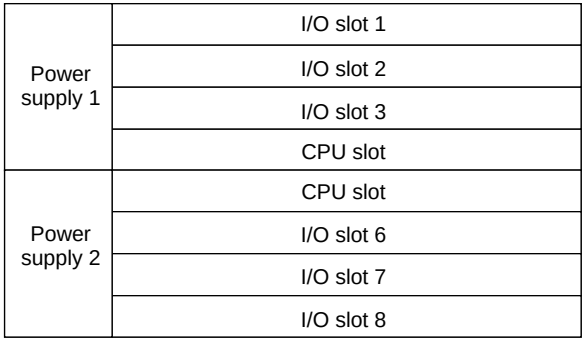
Many of the Run-Time CLI commands accept port numbers or IP addresses as arguments. The syntax for specifying port numbers and IP addresses is the same for all these commands.

Specifying port numbers

Each port number has two components: a slot number and a position number. The slot number identifies the chassis slot containing the I/O module that the port is on. The position number identifies the position of the port on the I/O module. Ports are always numbered from left to right beginning with 1 for the far left port.

In the Passport 1200 Switch, chassis slots are numbered from the top slot down, beginning with 1. Figure 8 on page 74 shows how the slots and ports in a Passport 1200 chassis are numbered.

Figure 8 Passport 1200 slot and port numbering



In the Passport 1100 Switch or the Passport 1150 Switch, the left I/O slot is slot 1, the right I/O slot is slot 2, and the fixed chassis ports are identified as belonging to slot 3.

To specify a single port number, type the slot number, a forward slash, and then the position number:

<slot>/<position>

For example, to specify the fourth port from the left on the third I/O module in the Passport 1200 chassis, the port number is:

```
3/4
```

To specify a list of port numbers, separate individual port numbers with commas:

<slot>/<position>,<slot>/<position>,<slot>/<position>

Notice that there is no space between the port numbers and the commas. Some examples of port lists are:

```
3/4,6/4,7/2
6/1,2/7,1/3
```

To specify a range of ports, type the low port number in the range, a dash, and then the high port number in the range:

```
<slot>/<position>-<slot>/<position>
```

Note that there are no spaces between the port numbers and dashes.

Some examples of port ranges are:

```
3/1-3/6
2/2-2/9
2/5-3/5
```

When you specify ports, you can specify any combination of port lists and port ranges. For example, the following port arguments are valid:

```
2/7,6/1-6/6
3/2-3/5,1/1-1/7,6/1
7/6,2/5,3/1-3/7,6/1
```

Specifying IP addresses and subnet masks

All IP addresses in the CLI are specified in dotted-decimal notation as follows:

```
<xxx>.<xxx>.<xxx>.<xxx>
```

An IP address with a subnet mask can be specified in two forms:

```
<xxx>.<xxx>.<xxx>.<xxx>/<yyy>.<yyy>.<yyy>.<yyy>
```

or

```
<xxx>.<xxx>.<xxx>.<xxx>/<n>
```

where:

xxx.xxx.xxx.xxx is the IP address in dotted-decimal notation.

yyy.yyy.yyy.yyy is the subnet mask in dotted-decimal notation.

n is the number of subnet mask bits.

The following examples refer to the same IP address and subnet mask pair:

```
10.10.10.1/255.255.255.0
10.10.10.1/24
```

Accessing the Run-Time CLI

To access the Run-Time CLI, log on to the switch using a Telnet connection from a terminal that has access to the Passport 1000 Series chassis. When you enter the CLI, the name of the system is the displayed prompt. For example:

```
Passport-1100>
```

To open a Telnet session from Passport Device Manager, click the Telnet icon from the tool bar.

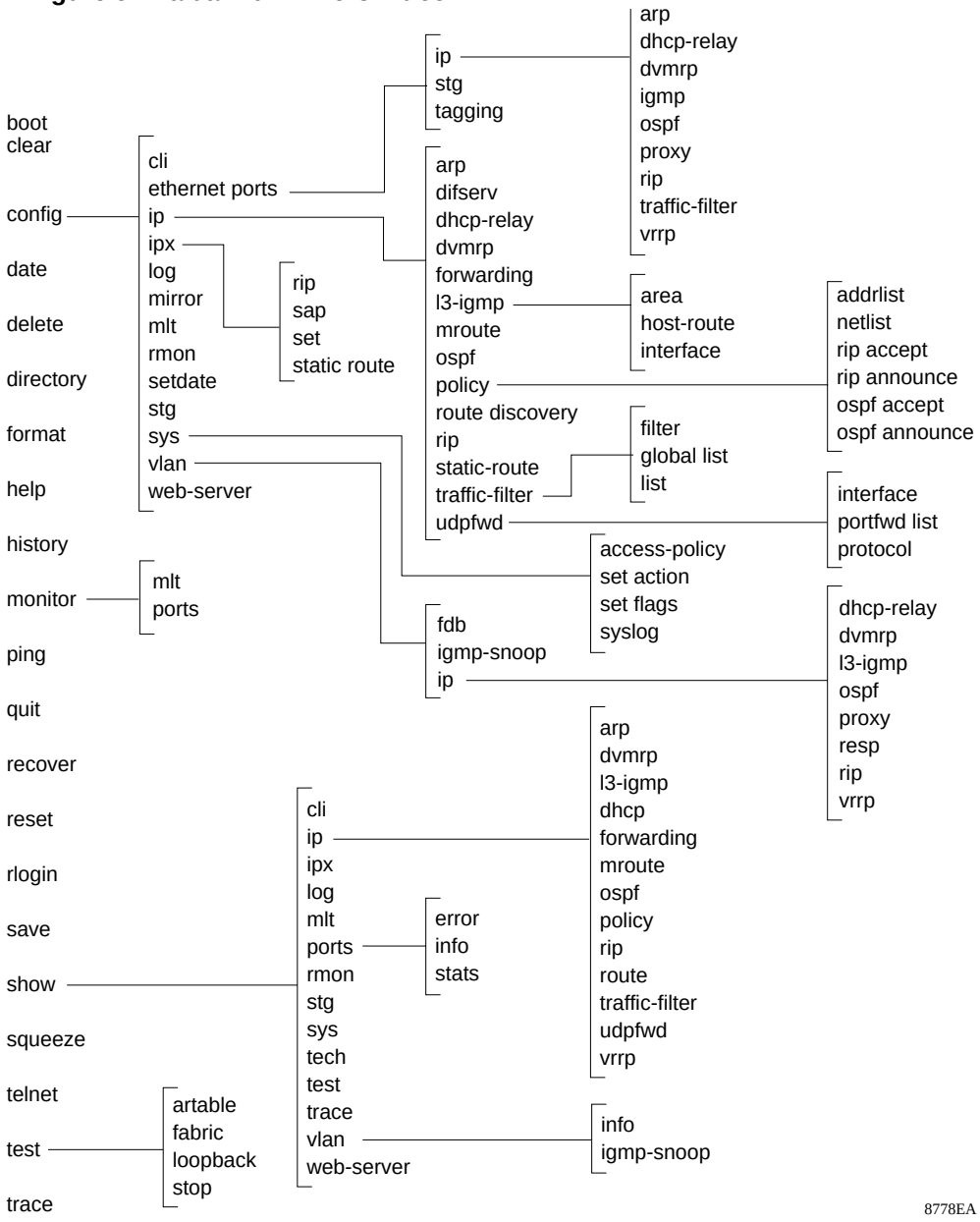
Run-time command list tree

Figure 9 shows an outline diagram of the main command groups in the Run-Time CLI tree. Appendix A, “CLI command list,” contains an alphabetical list of the Run-Time CLI commands. Other chapters in this manual list and describe the commands according to their function:

- Chapter 4, “Configuring switch management”
- Chapter 5, “Configuring layer 2 features”
- Chapter 6, “Configuring layer 3 protocol features”
- Chapter 7, “Configuring IP flow, policies, and filters”
- Chapter 8, “Monitor commands”

The remainder of this chapter describes the general CLI commands.

Figure 9 Partial Run-Time CLI tree



Navigation commands

The following navigation commands are available using the Passport Run-Time CLI:

Navigation command	Meaning
syntax	Displays all commands available at this level on the CLI tree.
back	Takes you back one level.
box	Returns to the top or box level.
cwc	[..]—changes the current working context.
pwc	Prints the current working context.
toplevel	Returns to the top level.
..	Goes back one level (same as the back command).

General commands

The following general commands are available in the Passport Run-Time CLI:

General command	Meaning
boot	Reboots the system (page 79).
clear	Clears statistics or flushes entries from a table (page 80).
date	Displays the calendar time. The command is valid only on Passport switches with a real-time clock (page 81).
help	Lists the commands in the CLI or displays syntax information for a specific command (page 81).
history	Lists the commands you have already entered in the current CLI session and lets you modify and reenter commands (page 84).
login/exit/quit/logout	Ends the CLI session or allows you to change the access level (page 85).

General command	Meaning
ping	Tests the network connectivity between the switch and another networking device (page 85).
pingipx	Tests IPX network connectivity (page 85).
reset [-y]	Resets the Passport 1000 Series switch (page 86).
traceroute	Allows you to trace the route to a remote host (page 87).

Boot command

The **boot** command reboots the Passport 1000 Series chassis with an image and configuration file or choices. The optional parameters of the command let you specify the boot source (flash, PCMCIA card, or TFTP server) and file name.

The syntax for the **boot** command is:

```
boot [<devfile>] [config <value>] [ip <value>] [file
<value>]
```

where:

devfile is the boot image.
{flash|pcmcia|config|nvram|tftp|trace|nic [filename]}

config <*value*> is the boot source.
{none|flash|pcmcia|net|skip|nvram|config [:filename]}

ip <*value*> is the IP address of the TFTP server, if booting from the server.

file <*value*> is the TFTP file to boot.

If you do not specify a device and file, the CLI uses the software and configuration files on the primary boot device.

Boot using a configuration script file

An extension of the **boot** command allows you to use an ASCII-based text file containing CLI commands to configure a Passport switch. When using this option, the switch boots using the factory default mode. The CLI commands contained in the configuration script are applied against the default configuration.

The script file is an ASCII text file. The first line of the file must include a pound sign (#) followed by a carriage return, with the remaining lines containing valid CLI commands, one per line.

Using a configuration script that resides on the flash file system, the command format is:

boot <*bootdevice*> [:bootfile>] config
[flash|pcmcia]:<*configscriptname*>

For example:

```
Passport# boot flash:2 config flash:config_script.txt
```

Clear commands

The clear commands are used to clear statistics from counters, or to flush entries from a table. These commands use the parameters port (the port number) and vid (the VLAN ID).

The **clear** commands include the following options:

clear followed by:	
ip arp ports <*port*>	Clears ARP port entries from the ARP table.
ip arp vlan <*vid*>	Clears ARP VLAN entries from the ARP table.
ip route ports <*port*>	Clears route entries associated with the specified port.
ip route vlan <*vid*>	Clears route entries associated with the specified VLAN.

clear followed by:	
`igmp-snoop groups [<vid>]`	Clears the dynamically learned multicast group members.
`igmp-snoop mrouter [<vid>]`	Clears the learned multicast router ports.
`ports stats [<ports>]`	Clears port statistics from the switch counters.

Date command

The **`date`** command is available only when the switch real-time clock is set. Not all Passport switches have real-time clocks. The **`date`** command displays the calendar time in the format: day of the week, month, hh:mm:ss, year. If the **`date`** command is entered on a device that does not have a real-time clock, the following message is displayed:

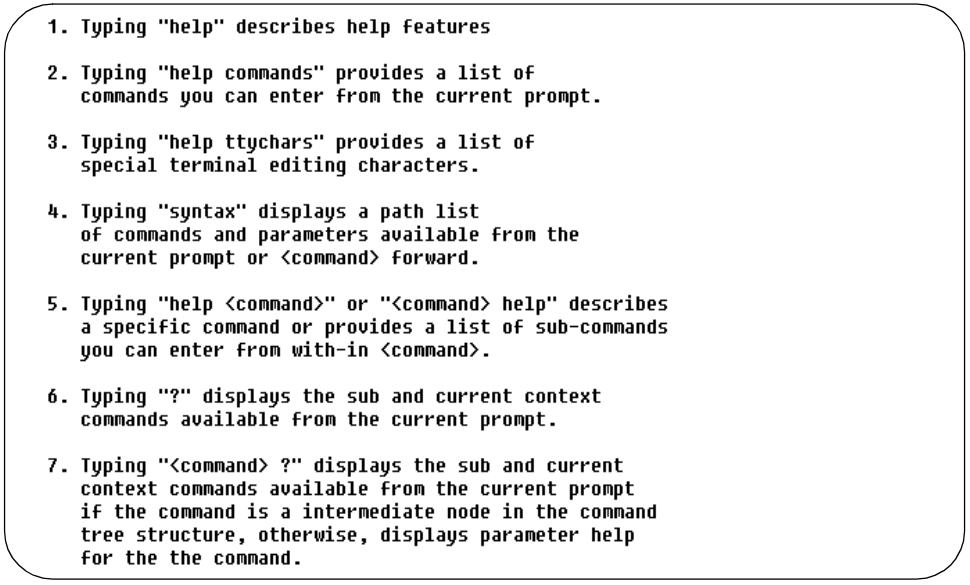
```
The Real Time Clock is not present.
```

Use the **`config setdate`** command to set the real-time clock.

Help command

Online help is available in the Passport 1000 Series Run-Time CLI. Use the **`help`** command to see the available types of online Help (Figure 10).

Figure 10 Passport 1000 Series online Help


1. Typing "help" describes help features
2. Typing "help commands" provides a list of commands you can enter from the current prompt.
3. Typing "help ttychars" provides a list of special terminal editing characters.
4. Typing "syntax" displays a path list of commands and parameters available from the current prompt or <command> forward.
5. Typing "help <command>" or "<command> help" describes a specific command or provides a list of sub-commands you can enter from with-in <command>.
6. Typing "?" displays the sub and current context commands available from the current prompt.
7. Typing "<command> ?" displays the sub and current context commands available from the current prompt if the command is a intermediate node in the command tree structure, otherwise, displays parameter help for the the command.

To see a list of all commands available at the current login access level, type **`help commands`** at the prompt. Figure 12 on page 84 shows the help commands with read/write/all access in the Run-Time CLI. Not all of these commands are available at all login access levels.

Figure 11 help command output in the Run-Time CLI

```
back            back up one level
boot            boot the system with an image and configuration file or choices
box             go to top or box level
clear           clear configuration commands
config          configuration commands
copy            copy a file to a device
cwc             change current working level
date            display calender time
delete          delete a file from a device
directory       list files on a device
exit            logout of system
format          format a device
help            display help about cli commands
history         show command history
login           re-login to a different access level
logout          logout of system
monitor         display switch configuration in time interval
ping            ping an ip address
pingipx         ping IPX address
pwc             print current working level
quit            logout of system
recover         recover deleted files on a device
reset           reset the system
rlogin          rlogin to a remote host
rsh             execute a shell command on a remote machine
save            save running configuration to a file or nvram
show            display switch configuration
squeeze         reclaim deleted file space on a device
telnet          telnet to a remote host
test            test the switch
toplevel        go to top level
trace           trace file configuration commands
traceroute      trace route to a remote host
..              back up one level
```

If you use the **help** command followed by a specific command (`help [<command>]`), a description of the command with a list of subcommands or required and optional parameters is displayed. Figure 12 shows the output for the **help config** command.

Figure 12 help config command output

```
Configuration cli commands
cli             cli configuration commands
ethernet        ethernet port configuration commands
info            show current level parameter settings and next level directories
ip              ip protocol configuration
ipx             IPX configuration commands
log             system log file commands
mirror          port mirroring commands
mlt             Multi-link trunking commands
radius          radius protocol configuration
rmon            remote monitor commands
setdate         Set calendar time. Out of range input will be automatically wrap
 around.
stg             spanning tree commands
sys             system configuration commands
vlan            vlan configuration commands
web-server      web server commands
```

History commands

The Run-Time CLI **history** commands let you list the commands you have entered during the current session. They also allow you to reenter commands.

The **history** commands include the following options:

history followed by:	
history	Lists the commands that you have entered during the current CLI session.
!!	Reenters the most recently entered command.
!<number> : run command <number>	Enters the command identified in the command history by the variable <number>.
!<str>	Runs the last command that matches the given string <str>.
!?<substr>	Runs the last command that matches the given substring <substr>.
^<sstr>^<rstr>	Enters the most recent command but substitutes a new string for a given string.

Figure 13 shows output for the **history** commands in the Run-Time CLI.

Figure 13 history command output

```
history commands substitution syntax
  !!  : run last command
  !<number> : run command <number>
  !<str> : run last command that matches <str>
  !?<substr> : run last command that matches <substr>
  ^<sstr>^<rstr> : replace <sstr> with <rstr> in last command
```

Login/exit/logout/quit commands

The **exit**, **quit**, and **logout** commands are used to close a CLI session or to change the access level. Use the **login** command to log in to the system.

Note: If you make configuration changes during a CLI session, save the changes in the configuration file. For information about saving changes, see page 89.

Ping and pingipx commands

The Run-Time CLI **ping** command tests the network connection to another networking device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. If the device receives the packet, it sends a ping reply. When the switch receives the reply, it displays a message indicating that the specified IP address is active. If no reply is received, a message indicates that the address is not responding.

The command syntax for the **ping** command is:

```
ping <ipaddr> [<datasize>] [<count>] [-s] [-I <value>] [-t
<value>] [-d]
```

where:

ipaddr is the IP address of the other networking device.

datasize is the size of the ping data (16 to 4076).

count is any integer value equal to or greater than 1 (from 1 to 9999). The default is 1.

`[-s]` is a continuous ping at the interval rate.

`[-I <value>]` is the interval between transmissions in seconds (1 to 60).

`[-t <value>]` is the no answer timeout value in seconds (1 to 120).

`[-d]` is the set ping debug.

Figure 14 shows output for the **`ping`** command.

Figure 14 ping command output

```
PING 10.10.40.169: 56 data bytes
64 bytes from 10.10.40.169: icmp_seq=0. time=2 ms
ping: timeout
----10.10.40.169 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/2
```

The **`pingipx`** command tests an IPX network connection using the syntax:

`pingipx <ipxhost> [<count>] [-s] [-q] [-t <value>]`

where:

`ipxhost` is the IP address net node.

`count` is the number of times to ping the host (1 to 9999).

`-s` is a continuous ping.

`-q` is quiet output (same as non-verbose mode).

`-t value` is the no-answer timeout value in seconds (1 to 120).

Reset command

The **`reset`** command resets the Passport 1000 Series switch and uses the most recently saved configuration file to reload the system parameters.

Traceroute command

The **traceroute** command traces a route to a remote host and is used primarily for troubleshooting. It shows the routes that are used, or it indicates from which route it can go no further if the remote network is not reachable.

The command syntax is:

```
traceroute <ipaddr> [<datasize>] [-m <value>] [-p <value>]
[-q <value>] [-w <value>] [-v]
```

where:

ipaddr is the IP address of the switch.

datasize is the probe packet size (1 to 1464).

-m <*value*> is the maximum time-to-live (TTL) value (1 to 255).

-p <*value*> is the base UDP port number (0 to 4294967295).

-q <*value*> is the number of probes per TTL (1 to 255).

-w <*value*> is the wait time per probe (1 to 255).

-v is verbose mode (showing all).

Figure 15 shows output for the **traceroute** command.

Figure 15 traceroute command output

```
traceroute to 134.177.1.22, 30 hops max, 40 byte packets
 1  * 10.10.40.1  4 ms *
 2  * 10.10.11.1  2 ms *
 3  * 134.177.181.1  2 ms *
 4  134.177.180.1  5 ms 3 ms 3 ms
 5  134.177.184.2  2 ms 3 ms 2 ms
 6  * 134.177.103.2  3 ms *
 7  * * *
 8  * * 134.177.1.22  3 ms
```

File and device management commands

The file and device management commands enable you to manage files on the flash module, the PCMCIA card, or the network. These commands operate the same way as the boot monitor CLI commands.

The file management commands include the **`log`** and **`trace`** commands, as well as the following options:

`copy <srcdevfile> <destdevfile> [debug]`	Copies a file from one device to another. • *`srcdevfile`* is the source device (flash, PCMCIA, configuration, TFTP, etc.) and file name. • *`destdevfile`* is the destination device and file name. • `[debug]` allows you to debug the CLI script output.
`delete <devfile>`	Deletes a file from a boot device. • *`devfile`* is the destination device and file name.
`directory <devfile>[-l]`	Lists the files on a boot device. • *`devfile`* is the destination device and file name. • `-l` *`value`* is the user login name {string}.
`format <device> [-y]`	Formats the flash module or PCMCIA card. • *`device`* is flash or PCMCIA.
`recover <device>`	Recovers files marked for deletion from the flash module or PCMCIA card. • *`device`* is flash or PCMCIA.
`rsh <ipaddr> -l <value> <cmd>`	Executes a shell command on a remote machine. • *`ipaddr`* is the IP address. • `-l` *`value`* is the user login name {string}. • *`cmd`* is the command to execute on remote host {string}.
`squeeze <device>`	Reclaims space occupied by files marked for deletion on the flash module. • *`device`* is flash or PCMCIA.
`telnet [<ipaddr>]`	Sets up a Telnet session to a remote device. • *`ipaddr`* is the IP address.

`rlogin [<ipaddr>]`	Allows remote login to a remote device. • *ipaddr* is the IP address.
`save [<devfile>] [standby]`	Saves your configuration. • *devfile* is the destination device and file name. • [standby] is the standby or backup destination (for example, standby NVRAM).

Figure 16 shows output for the file and device management commands.

Figure 16 file and device management commands output

```
Passport-1100# dir
Device: flash
FN Name                                Flags    Length
-- ----                                -----    ------
1  acc2.x.x                              XZN    994730
2  syslog                                 LN    131072
3  acc2.x.y                              XZN    1264023
4  accboot2.x.x                          XZN    87345
5  accbootx.x.z                          XZN    87884
6  config2xx                              CN    60080
--                                             ------
6   files          bytes used=  2818048 free=1376256
Passport-1200# copy flash:acc2.x.x pcmcia:newfile
programming ... pcmcia:newfile as file# 2 994730 bytes
Passport1100# dir
Device: flash
FN Name                                Flags    Length
-- ----                                -----    ------
1  acc2.x                                XZN    994730
2  syslog                                 LN    130896
--                                             ------
2   files                          bytes
used=  1114112 free=3080192
Device: pcmcia
FN Name                                Flags    Length
-- ----                                -----    ------
1  acc2.x.x                              XZN    994730
2  newfile                               XZN    994730
--                                             ------
2   files                          bytes
used=  2097152 free=2097152
Passport-1100# delete flash:acc2.x.x
File [flash:acc.2.x] deleted
Passport-1100# squeeze flash
recovering deleted file space ... success
Passport-1100# dir
Device: flash
FN Name                                Flags    Length
-- ----                                -----    ------
1  syslog                                LN    130896
--                                             ------
1  files                          bytes
```

```
used=  131072 free=4063232
   Device: pcmcia
   FN Name                                Flags    Length
   -- ----                                -----    ------
   1  acc2.x.x                              XZN    994730
   2  newfile                               XZN    994730
   --                                               ------
   2   files                          bytes
used=  2097152 free=2097152
```

Copying a script file to a running configuration

An extension of the **copy** command allows the switch to read a script file (an ASCII-based text file containing CLI commands) and execute the commands as if they were typed during a console session. It also allows you to copy a running configuration to a script file. By default, script execution does not display at the device where the command is issued. However, if the optional debug parameter is used, execution of the command in the script file and the results are output to the device from which the command was executed.

The first line of the script file must include a pound sign (#) followed by a carriage return. The remaining lines must contain valid CLI commands, one per line.

The command format is:

`copy <`*`sourcedevice:filename`*`> running-config [debug]`

where:

`sourcedevice` is a flash, PCMCIA, or TFTP-based file server. If “tftp” is specified, you are prompted for the server IP address and the file name.

`filename` is the name of the file to be copied.

`[debug]` is the optional parameter that allows you to view the script while it is executing.

Note: Use caution when executing script files from within the CLI. The command execution references from your current position in the directory structure.

Accessing files using the standby SSF module

On a Passport 1200 Switch, the latest Passport software allows you to access the standby SSF module from the active SSF module using **copy** and **telnet** command operations.

You can copy files in the flash file system of the active SSF module to the flash file system of the standby SSF module and vice versa, using the **copy tftp** command. The IP address used for the copy is 127.0.0. Slot is the slot number of the standby SSF module. In the Passport 1200 switch, this slot number is 4 or 5.

To copy a file from the active SSF module to the standby SSF module, use the `copy` *`device`*`:`*`filename`* `tftp` command from the active SSF module.

A Telnet session can be established from the active SSF module to the standby SSF module using the 127.0.0.*`slot`* address.

Test commands

The `test` commands enable you to test the switch while the switch is operating. The tests do not interfere with the normal bridging and routing activities of the switch, but they do occupy the CPU.

The **test** commands include the following options:

test followed by:	
`artable`	Runs the Address Resolution table test.
`fabric`	Tests the switch fabric of the switch.
`test loopback <`*`ports`*`> [<`*`int/ext`*`>]`	Places individual ports into internal or external loopback mode. *`ports`* is the port list {`slot/port[-slot/port][, ...]`}. `<int|ext>` is internal or external loopback mode defined by an ASCII string.
`stop artable`	Stops the current Address Resolution table test.
`stop fabric`	Stops the current switch fabric test.

test followed by:	
`stop loopback <ports>`	Stops the current loopback test.
`ports stats [<ports>]`	Clears port statistics from the switch counters.

Note: To test a port in loopback mode, the port must first be put into the testing state using the **`config ethernet`** *<port>* **`state test`** command. After completing the test, put the port back in normal mode using the **`config ethernet`** *<port>* **`state enable`** command.

show test commands

The **`show test`** commands provide information about tests that are run on the switch.

show test artable command

The **`show test artable`** command displays information about the AR table test results (Figure 17).

Figure 17 show test artable command output

```
Running a switch fabric test...
Current test results:

  IfIndex: 0
   Result: inProgress
PassCount: 1157687756
FailCount: 0
```

show test fabric command

The **`show test fabric`** (C Font) command displays the result of the latest switch fabric test (Figure 18).

Figure 18 show test fabric command output

```
Running a switch fabric test...
Current test results:

  IfIndex: 0
   Result: inProgress
PassCount: 1157719536
FailCount: 0
```

show test loopback command

The **`show test loopback`** command displays the results of the latest loopback test for the switch or for the specified port(s) in the format `show test loopback [<ports>]`. Figure 19 displays sample output for port 1/1.

Figure 19 show test loopback command output

```
Waiting for last test to clean up & exit.
Last test results:

     Port: 1/1
  IfIndex: 16
   Result: none
PassCount: 0
FailCount: 0
```

Trace commands

The **`trace`** commands allow you to see the status of the switch in a given time frame.

Note: Using the **`trace`** command slows the performance of your switch.

The **trace** commands use the following parameters:

trace followed by:	
`info [tail]`	Shows the trace message file. The `tail` option allows you to view the log from the back first.
`clear`	Clears tracing on a module.
`level [<modid>] [<level>]`	Sets the trace level on a module for the specified module ID. Use Help to see a list of ID numbers. The level is one of the following values: 0 = Disabled 1 = Very terse 2 = Terse 3 = Verbose 4 = Very verbose
`off`	Disables tracing on a module.
`screen [<setting>]`	Sets the trace display to screen on or off.

show trace commands

The **show trace** commands display trace information for the switch.

show trace file command

The **show trace file** command displays the trace message file when tracing is on.

The command syntax is:

```
show trace file [tail]
```

where:

`tail` displays the most recent entry first.

Figure 20 shows sample output for the **trace file** command.

Figure 20 show trace file command output

```
[000 00:00:00:366] rcStart MAIN: init.c    : 578 : System initialization
```

show trace level command

The **`show trace level`** command displays the current module ID numbers and trace levels.

Figure 21 shows output for the **`trace level`** command.

Figure 21 show trace level command output

```
usage: trace level <modid> <level>

Module IDs:              Trace Levels:
 0 - Common                0    0 - Disabled
 1 - SNMP Agent            0    1 - Very terse
 2 - RMON                  0    2 - Terse
 3 - Port Manager          0    3 - Verbose
 4 - Chassis Manager       0    4 - Very verbose
 5 - STG Manager           0
 6 - Phase2 OSPF           0
 7 - Hardware I/F          0
 8 - (N/A)                 0
 9 - CP Port               0
10 - (N/A)                 0
11 - VLAN Manager          0
12 - CLI                   0
13 - Main                  0
14 - Phase2 IP+RIP         0
15 - RCC IP                0
16 - HTTP Server           0
17 - ASIC I/F              0
18 - Gigabit               0
19 - Watch Dog Timer       0
20 - Topology Discovery    0
21 - (N/A)                 0
22 - (N/A)                 0
23 - IGMP                  0
24 - IPFIL                 0
25 - MLT                   0
27 - IPMC                  0
29 - DVMRP                 0
30 - P2IPX                 0
31 - RCIPX                 0
36 - RADIUS                0
```

Chapter 4
Configuring switch management

This chapter describes the CLI commands that you use to configure switch management functions in the Passport 1000 Series switch. The configuration (config) branch is a main branch in the CLI tree, used to access all the parameters in the switch.

The chapter includes the following sections:

- "show config command," next
- "show tech command" on page 100
- "CLI management commands" on page 101
- "Log commands" on page 105
- "RMON commands" on page 109
- "config setdate command" on page 110
- "System commands" on page 110
- "Syslog commands" on page 123
- "web-server commands" on page 125

show config command

The **`show config`** command displays the current switch configuration.

Note: N/A displayed in a **`show`** command output indicates that the value is not applicable.

Figure 22 shows partial output for the **`show config`** command.

Figure 22 show config command output

```
Passport 1100# show config
#
# box type             : Passport-1100
# boot monitor version : v2.1.0.0.b011
# software version     : REL2.1.0.0_B068
#

#
# HARDWARE CONFIGURATION
#

# slot 1
# slot 2
# slot 3        16x100BaseTXWG      ARU3         QUID5        PIC3
# ssf           1100                SQUID3       SWIP2        Xy2

#
# SYSTEM CONFIGURATION
#

config
cli
sys
set
        contact "support@baynetworks.com"
        snmp community l1 private
        snmp trap-recv 10.10.40.91 v1 public
        snmp trap-recv 10.10.40.92 v1 public
        snmp trap-recv 10.122.60.182 v1 optivity90_autotrap
        snmp trap-recv 10.122.60.188 v1 superagent_autotrap
        snmp trap-recv 134.177.25.24 v1 public
        snmp trap-recv 134.177.25.49 v1 public
        snmp trap-recv 134.177.25.61 v1 public
        snmp trap-recv 134.177.25.78 v1 public
        snmp trap-recv 134.177.25.106 v1 public
        snmp trap-recv 134.177.25.170 v1 public
        snmp trap-recv 134.177.80.41 v1 public
        snmp trap-recv 134.177.80.101 v1 public
        snmp trap-recv 134.177.80.109 v1 public
        snmp trap-recv 134.177.80.113 v1 public
        snmp trap-recv 134.177.80.125 v1 public
        snmp trap-recv 134.177.80.126 v1 public
        snmp trap-recv 134.177.80.151 v1 public
        snmp trap-recv 134.177.80.156 v1 public
        snmp trap-recv 134.177.80.189 v1 public
        snmp trap-recv 134.177.80.208 v1 public
```

```
back
syslog
back

#
# LINK-FLAP-DETECT CONFIGURATION
#

link-flap-detect
back

#
# ACCESS-POLICY CONFIGURATION
#

access-policy
        enable true
policy 1
back
policy 50
        create
        name "jnm team"
back
policy 51
        create
        accesslevel rwa
        host 134.177.160.225
        name "test"
        username "jhsu"
        network 134.177.160.0/255.255.255.0
        service telnet enable
back
back

#
# DIAG ARU MONITOR CONFIGURATION
#

diag
back
back

#
# WEB CONFIGURATION
#
 web-server
         password rwa jnm jnm
 back

 #
 # RMON CONFIGURATION
 #

rmon enable

 #
 # TRAFFIC-FILTER CONFIGURATION
 #

ip
traffic-filter
        create global src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/0.0.0.0 id 3
filter 3
action
        mirror enable
back
match
        dst-port 0 dst-option equal
        src-port 0 src-option equal
```

show tech command

The **show tech** command displays system status technical information and outputs the following information:

- System information, such as location
- Chassis type and serial number
- Power supplies
- Fans
- Modules
- System errors
- Device information, such as boot sources and priority
- Port locks
- Topology status
- Software versions
- System performance
- VLAN information, such as numbers and port members
- Port information, such as type and status
- Route information
- OSPF information, such as area, interface, and neighbors
- Memory
- Interface
- Log and trace files

Figure 23 shows partial output for the **show tech** command.

Figure 23 show tech command output

```
Sys Info:
---------------


General Info :

        SysName      : Passport 1100
        SysUpTime    : 49 day(s), 18:12:27
        SysContact   : support@baynetworks.com
        SysLocation  : 4401 Great America Parkway, Santa Clara, CA 95052

Chassis Info :

        Chassis : 1100
        Serial# : 60252
        HwRev   : v3.0
        NumSlots: 3
        AruMode : AruThree
        EocMode : default

Power Supply Info :

        Ps#1 Status       : up
--More-- (q = quit)
```

CLI management commands

The CLI management commands allow you to view or change the CLI configuration. The commands include the following subsets:

- **`config cli general`** commands
- **`config cli password`** commands

config cli commands

The **`config cli`** commands are general management commands for the CLI and uses the following options:

`config cli` followed by:	
`banner add <string>`	Adds a login banner.
`banner default banner <true/false>`	Sets the login banner to default to true or false.
`banner delete`	Deletes the login banner.

config cli followed by:	
`banner info`	Displays the current banner settings.
`defaultlogin <true|false>`	Sets default login to default to true or false.
`defaultpassword <true|false>`	Sets default password to default to true or false.
`loginprompt <string>`	Adds a login prompt
`info`	Displays the current CLI settings (Figure 24).
`monitor duration <integer>`	Changes monitoring time duration (refresh rate) for the monitor commands (see Chapter 8, "Monitor commands"). The time duration is in seconds (1 to 1800).
`monitor info`	Displays the current setting for monitor duration and interval using the monitor commands.
`monitor interval <integer>`	Changes monitoring time interval between screen updates in seconds (1 to 600) using the monitor commands.
`more <true|false>`	*True* sets output display scrolling to one page at a time. *False* (default) sets output display to continuous scrolling.
`motd add <string>`	Adds a login "message of the day" (MOTD).
`motd displaymotd <true/false>`	Displays the current settings for the MOTD.
`motd delete`	Deletes the MOTD.
`motd info`	Displays the current MOTD settings.
`passwordprompt <string>`	Changes system password.
`prompt <prompt>`	Sets the root level prompt and sysName to the defined prompt name.
`rlogin-sessions <nsessions>`	Sets the allowable number of inbound remote CLI login sessions from 0 to 8; default is 8.
`screen lines <nlines>`	Sets the number of lines in the output display from 8 to 64; default is 23.
`telnet-sessions <nsessions>`	Sets the allowable number of inbound Telnet sessions from 0 to 8; default is 8.
`timeout <nseconds>`	Sets the idle timeout period before automatic logout for CLI sessions from 30 to 65535 seconds; default is 90 seconds.

Figure 24 config cli info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

               defaultlogin : true
            defaultpassword : true
                loginprompt : Login:
                       more : true
             passwordprompt : Password:
                     prompt : swlab-edge2
            rlogin-sessions : 8
               screen-lines : 23
            telnet-sessions : 8
                    timeout : 900
```

show cli commands

The **`show cli`** command outputs display information about the switch CLI configuration.

show cli info command

The **`show cli info`** command displays the CLI configuration.

Figure 25 shows output for the **`show cli info`** command.

Figure 25 show cli info command output

```
cli configuration

more            : true
screen-lines    : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout         : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : true
default login prompt        : Login:
custom login prompt         : Login:
use default password prompt : true
default password prompt     : Password:
custom password prompt      : Password:
```

show cli who command

The **show cli who** command displays who is logged in to the switch.

Figure 26 shows output for the **show cli who** command.

Figure 26 show cli who command output

```
SESSION   USER              ACCESS    IP ADDRESS
Telnet0   rwa               rwa       134.177.25.214
Console                     none
Modem                       none
```

config cli password commands

The **config cli password** commands allow you to view or change the login or password for the different access levels of the routing switch, where password is the password associated with the user name or login name. You must have read/write/all privileges in order to view or change passwords.

The command syntax is:

```
config cli password
```

The **config cli password** command uses the following options:

config cli password followed by:	
info	Displays current login and password settings.
ro <*username*> [<*password*>]	Sets the Read-Only login and/or password.
l1 <*username*> [<*password*>]	Sets the layer 1 login and/or password.
l2 <*username*> [<*password*>]	Sets the layer 2 login and/or password.
l3 <*username*> [<*password*>]	Sets the layer 3 login and/or password.
rw <*username*> [<*password*>]	Sets the read/write login and/or password.
rwa <*username*> [<*password*>]	Sets the read/write/all login and/or password.

Figure 27 shows output for the **config cli password info** command.

Figure 27 config cli password info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

        ACCESS    LOGIN           PASSWORD
        rwa       rwa             rwa
        rw        rw              rw
        l3        l3              l3
        l2        l2              l2
        l1        l1              l1
        ro        ro              ro
```

show cli password command

The **show cli password** command displays the CLI access, login, and password combinations.

Figure 28 shows output for the **show cli password** command.

Figure 28 show cli password command output

```
ACCESS    LOGIN           PASSWORD
rwa       rwa             rwa
rw        rw              rw
l3        l3              l3
l2        l2              l2
l1        l1              l1
ro        ro              ro
```

Log commands

The **log** commands configure and display the switch log files.

config log commands

The **config log** commands allow you to show, write, or clear the log file created automatically by the system. The **config log** commands use the following syntax and options:

config log followed by:	
info	Displays current log settings (Figure 29).
clear	Clears the log file.
level [<*level*>]	Shows and sets the log level to one of the following values: 0 = Information 1 = Warning 2 = Error 3 = Manufacturing 4 = Fatal
screen [<*setting*>]	Sets the log display on the screen on or off {off|on}.
write <*str*>	Writes the log file with the designated string, where string is the string or command that you append to the log file. If the name contains spaces, you must enclose it in quotation marks.

Figure 29 shows output for the **config log** command.

Figure 29 config log command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                      clear : N/A
                      level : 0
                     screen : off
                      write : N/A
```

The log file is composed of two halves. Each half is an integral number of device sectors (the default is 1). Each log record is 256 bytes long. The logger subsystem writes to the “current” half. When a half fills up, it swaps over to the other half, clearing it if necessary.

When a switch boots, the following log message is displayed:

```
flash:syslog:0:3
```

where:

`flash` is the storage media.

`:syslog` is the file name on storage media.

`:0` is the zero half.

`:3` is the third entry for the current half.

The log file used when the switch boots is the last (or highest file number) log file. If the flash file system is full, it attempts to copy the log file to the PCMCIA card (optional). You can copy the log file. The next time the switch resets, it uses the highest file number of the log file.

show log commands

The **`show log`** commands display switch log information.

show log file command

The **`show log file`** command displays the log file automatically created by the system.

The command syntax is:

```
show log file [tail]
```

Figure 30 is a sample display, where the `[tail]` parameter is entered to configure the display to enter the most recent information first. If your Passport switch has a real-time clock, the log file shows real time.

Figure 30 show log file tail command output

```
Passport 1100# show log file tail
 389: [000 12:58:53:778] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 388: [000 12:58:51:794] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 387: [000 15:47:23:566] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 386: [000 15:47:21:082] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 385: [000 15:46:01:049] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 384: [000 15:45:58:566] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 383: [000 13:59:35:466] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 382: [000 13:59:32:982] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 381: [000 13:58:59:966] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 380: [000 13:58:57:966] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 379: [000 13:58:57:466] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 378: [000 07:15:09:400] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 377: [000 07:15:06:900] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 376: [000 07:07:01:900] INFO: Code=0x0 Task=tTrapd: Link Up(3/9)
 375: [000 07:06:59:900] INFO: Code=0x0 Task=tTrapd: Link Down(3/9)
 374: [000 04:20:55:300] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 373: [000 04:20:52:800] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 372: [000 05:41:57:755] INFO: Code=0x0 Task=tTrapd: Link Up(3/9)
 371: [000 05:41:55:755] INFO: Code=0x0 Task=tTrapd: Link Down(3/9)
 370: [000 05:41:26:255] INFO: Code=0x0 Task=tTrapd: Link Up(3/10)
 369: [000 05:41:24:255] INFO: Code=0x0 Task=tTrapd: Link Down(3/10)
 368: [000 05:36:09:755] INFO: Code=0x0 Task=tTrapd: Link Up(3/9)
 367: [000 05:36:07:255] INFO: Code=0x0 Task=tTrapd: Link Down(3/9)
--More-- (q = quit)
```

show log level command

The **`show log level`** command displays the level of information being entered in the log (Figure 31). The level ranges from information (INFO), where all messages are entered, to FATAL, where only fatal errors are recorded. The manufacturing (MFG) level is for manufacturing purposes only and not available for customer use.

Figure 31 show log level command output

```
Log Levels are:
 0 = INFO
 1 = WARNING
 2 = ERROR
 3 = MFG
 4 = FATAL
The Log Level is INFO
```

RMON commands

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on your Passport switch and an RMON management application, such as Device Manager. Although it is currently necessary to use Device Manager to configure RMON on your switch, the CLI has limited RMON capability.

config rmon commands

The **config rmon** commands enable, disable, and display RMON status on the switch.

The **config rmon** commands include the following options:

config rmon followed by:	
info	Indicates if RMON is enabled or disabled.
disable	Disables RMON.
enable	Enables RMON.

show rmon command

The **show rmon** command displays the status of RMON on the switch.

Figure 32 shows output for the **show rmon** command.

Figure 32 show rmon command output

```
RMON Info :

        Status       : off
        MemorySize   : 250000
        SaveConfig   : false
```

config setdate command

The **config setdate** command sets the calendar time in the format: day of the week, month, day, hh:mm:ss, year. This command is valid only on the Passport switches with real-time clocks. If the switch does not have a real-time clock, issuing a **date** or **setdate** command results in the message:

```
The real time clock is not present.
```

The **config info** command displays the status of the **config setdate** command.

System commands

The system commands manage the switch and allow you to view system settings. The **config sys info** command displays current configuration information.

The following are the system command subtopics:

- "Access policy commands" on page 110
- "config sys set action commands" on page 114
- "config sys set flags commands" on page 115
- "Other config sys set commands" on page 117
- "show sys commands" on page 119
- "Syslog commands" on page 123

Access policy commands

Access policies allow you to control management access by setting policies for services to prevent or allow access to the switch. You can specify which hosts or networks can access the switch through Telnet, SNMP, HTTP, rsh, and rlogin and whether the mode allows or denies access.

config sys commands

Use the **config sys** commands to enable and disable the Telnet client and TFTP server.

Command	Description
telnet-client <*enable*|*disable*>	Enables and disables the Telnet client.
tftp server <*enable*|*disable*>	Enables and disables the TFTP server.

config sys access-policy commands

Use the **config sys access-policy** commands to get information about, or to enable, access policies on the switch.

Command	Result
info	Displays the global access policy setting - enabled or disabled.
enable <true|false>	Globally enables or disables the IP access policy feature on the switch. If set to *false*, no policies are applied.

config sys access-policy policy commands

The **config sys access-policy policy** commands configure specific policy IDs (where *pid* is from 1 to 65535) and use the following syntax and options:

config sys access-policy policy <pid> followed by:	
info	Displays characteristics of the specified access policy (Figure 33).
access level <*level*>	Sets policy access level, where *level* is policy access level {ro|rw|rwa}, or read-only, read/write, read/write/all.
create	Creates a new access policy with a policy ID from 1 to 65535.

config sys access-policy policy <pid> followed by:	
`delete`	Deletes the access policy with a specified policy ID (1 to 65535).
`disable`	Disables the specified access policy (1 to 65535).
`enable`	Enables the specified access policy (1 to 65535).
`host <ipaddr>`	Sets the access policy trusted host address. Applicable only for remote login and remote shell execution and is the IP address `{a.b.c.d}` of the host used to authenticate the user. The login must be the specified user at the specified host for access.
`mode <mode>`	Defines the specified access policy mode as allow or deny access.
`name <name>`	Sets the specified access policy name `{string}`.
`network <addr|mask>`	Sets the access policy network address and subnet mask `{a.b.c.d/x | a.b.c.d/x.x.x.x | default]`.
`precedence <precedence>`	Sets the access policy precedence. The precedence determines which policy to use if multiple policies apply. The precedence range is from 1 to 128, with the lowest number having the highest precedence.
`service http <enable|disable>`	Enables or disables the specified access policy for HTTP service.
`service rlogin <enable|disable>`	Enables or disables the specified access policy for rlogin service.
`service snmp <enable|disable>`	Enables or disables the specified access policy for SNMP service.
`service telnet <enable|disable>`	Enables or disables the specified access policy for Telnet service.
`username <string>`	Sets the trusted host user name `{string}` from the trusted host for the specified policy. Applies only to rlogin access.

Figure 33 config sys access-policy policy command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                      create :
                      delete : N/A
                 accesslevel : readWrite
               policy enable : true
                        host : 0.0.0.0
                        mode : allow
                        name : default
                     network : 0.0.0.0/0.0.0.0
                  precedence : 128
                    username : none
```

Figure 34 shows the procedure for preventing a host from using specific services on a Passport switch. When denying services to a host, you must specify which service to enable for that policy PID.

Figure 34 deny access command output

```
Passport 1100# config sys access-policy enable true
Passport 1100# config sys access-policy policy 2 create
Passport 1100# config sys access-policy policy 2 name policy2
Passport 1100# config sys access-policy policy 2 enable true
Passport 1100# config sys access-policy policy 2 host 10.125.200.25
Passport 1100# config sys access-policy policy 2 mode deny
Passport 1100# config sys access-policy policy 2 service rlogin enable
Passport 1100# config sys access-policy policy 2 service http enable
Passport 1100# config sys access-policy policy 2 service snmp enable
```

The host 10.125.200.35 will not have switch access to HTTP, SNMP, and rlogin.

show sys access-policy info command

The **`show sys access-policy info`** command displays information about the specified access policy, or all access policies on the switch. In Figure 35, the policy created in the example above is displayed.

The command syntax is:

```
show sys access-policy info [<polname>]
```

Figure 35 show sys access-policy info command output

```
 AccessPolicyEnable: off

                Id: 1
              Name: default
       PolicyEnable: true
              Mode: allow
           Service: http|telnet|snmp
        Precedence: 128
           NetAddr: 0.0.0.0
           NetMask: 0.0.0.0
    TrustedHostAddr: 0.0.0.0
TrustedHostUserName: none
       AccessLevel: readWrite
             Usage: 0

                Id: 2
              Name:
       PolicyEnable: true
              Mode: allow
           Service: ftp
        Precedence: 10
           NetAddr: 0.0.0.0
           NetMask: 0.0.0.0
    TrustedHostAddr: 0.0.0.0
TrustedHostUserName:
       AccessLevel: readWrite
             Usage: 0
```

config sys set action commands

The **`config sys set action`** commands set system action using the following options:

`config sys set action` followed by:	
`info`	Displays the current settings (Figure 36).
`checkswinflash`	Runs checksum on the software version stored on the flash module.
`checkswinpcmcia`	Runs checksum on the software version stored on the PCMCIA card.
`cpuswitchover [-y]`	Resets the switch to change over to the backup CPU.
`getstandbycpuinfo`	Gets information about the standby CPU card (the redundant SSF module in a Passport 1200 Switch).

config sys set action followed by:	
`resetconsole`	Reinitializes the hardware UART drivers. Use only if the console or modem connection is hung.
`resetcounters [-y]`	Resets all the statistics counters in the routing switch to zero.
`resetmodem`	Resets the modem port.
`savetostandbynvram`	Sets the switch to save the switch configuration to backup CPU NVRAM.

Figure 36 config sys set action command output

```
Sub-Context: clear config monitor show test trace
Current Context:

              checkswinflash :
            checkswinpcmcia :
              cpuswitchover :
          getstandbycpuinfo :
               resetconsole :
              resetcounters :
                 resetmodem :
         savetostandbynvram :
```

config sys set flags commands

The **`config sys set flags`** commands set system flags to true or false for the following actions:

- Autoboot
- Using the configuration file after rebooting
- Isolating ports
- Activating debug mode

The **config sys set flags** commands include the following options:

config sys set flags followed by:	
info	Displays the current flag settings (Figure 37).
autoboot <*true*|*false*>	Controls whether the routing switch automatically runs the run-time image after being reset or stops at the monitor > prompt. Setting autoboot to false is useful for some debugging tasks. The default setting is true.
factorydefault <*true*|*false*>	Sets the switch configuration to factory default settings.
switchportiso <*true*|*false*>	Controls whether the ports operate in isolated mode. In isolated mode (true), the ports are members of the unassigned (isolated) VLAN instead of the Default VLAN, which includes all ports. The default is false.
debugmode <*true*|*false*>	Controls whether the routing switch automatically reboots following a fatal error. If true, the switch is not rebooted following a fatal error. If false, the switch is automatically rebooted following a fatal error. The default is false.
highpriomode <*true*|*false*>	Enables high-priority switching. A Passport switch can operate in either of two modes: Best Effort or Priority mode. The factory default setting is Best Effort mode, where all traffic is treated with the same priority. In Priority mode, high-priority traffic flows through the switch fabric using a high-priority data path; output buffers are reserved for high-priority traffic.

Figure 37 config sys set flags info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                    autoboot : true
               factorydefault : false
                switchportiso : false
                    debugmode : false
                 highpriomode : false
```

Note: When using the **config sys set flags** commands, type "save" to save the changes and reboot the switch. The changes take effect once the switch is rebooted.

Other config sys set commands

The **`config sys set action`** and **`config sys set flags`** commands include the following system set commands and options:

`config sys set` followed by:	
`info`	Displays current settings (Figure 38).
`boot <primary|secondary|tertiary> <choice>`	Sets the boot choice for the switch.
`config <choice>`	Sets the switch configuration `choice` to be `{none|flash|pcmcia|net|skip|nvram|config| [: filename]}`.
`contact <contact>`	Sets the contact for the switch `(ASCII string)`.
`eoc-mode <eocmode>`	Sets enforce operational configuration (eoc) mode {default|aru1quid4|aru 2quid4|aru3quid5} . By default, the switch operates in the mode of the lowest version ASIC present in any module. If you replace a module with a lower version, the entire switch operates with the functionality of the lower version. This command allows you to lock in a mode of operation. Then, if a lower version of the module is inserted, error messages will indicate that the module is not operable. (See **Note** on page 118.)
`location <location>`	Sets the location for the switch (ASCII string).
`name <prompt>`	Sets the box or root level prompt name for the switch (ASCII string).
`portlock <on|off>`	Turns the port locking on or off.
`sendtrap <true|false>`	Sets whether to send authentication failure traps.
`snmp community <ro|l1|l2|l3|rw|rwa> <commstr>`	Sets the SNMP community string for the selected community: `ro` is read-only. `rw` is read/write. `l2` is layer 2 read/write. `l3` is layer 3 (and layer 2) read/write. `rwa` is read/write/all.

config sys set followed by:	
`snmp trap-recv <ipaddr> <v1|v2c> <commstr>`	Sets an SNMP trap receiver, where: `<ipaddr>` is the IP address `{a.b.c.d}`. `<v1|v2c>` is the version; select version 1 or version 2c. `<commstr>` is the input community string `{string}`.
`topology <on|off>`	Turns topology on or off.
`snmp info`	Displays current SNMP settings (Figure 39).

Note: Some features require specific hardware versions: -A (ARU2) or -B (ARU3). If there is a -A or lower module installed in the switch, in order to utilize a feature requiring ARU3, you must remove the module or set eoc status to aru3quid5, which allows you to utilize ARU3 features but leaves the lower version module inoperable.

Figure 38 config sys set info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                        boot :
                               primary - flash 3
                             secondary - flash acc21newb15
                              tertiary - flash acc21newb15
                                 config - flash 2
                     contact : edwin
                    location : 4401 Great America Parkway, Santa Clara, CA 95052
                        name : swlab-edge2
                    portlock : on
                    sendtrap : false
                    topology : on
                    eoc-mode : default
```

Figure 39 config sys set snmp info command output

```
Passport 1100# config sys set snmp info

Sub-Context: clear config monitor show test trace
Current Context:

                  community :
                                  ro - public
                                  l1 - private
                                  l2 - private
                                  l3 - private
                                  rw - private
                                 rwa - secret
                  trap-recv :
                10.10.40.91 - v1 public
                10.10.40.92 - v1 public
              10.122.60.182 - v1 optivity90_autotrap
              10.122.60.188 - v1 superagent_autotrap
              134.177.25.24 - v1 public
              134.177.25.49 - v1 public
              134.177.25.61 - v1 public
              134.177.25.78 - v1 public
             134.177.25.106 - v1 public
             134.177.25.170 - v1 public
              134.177.80.41 - v1 public
             134.177.80.101 - v1 public
             134.177.80.109 - v1 public
             134.177.80.113 - v1 public
             134.177.80.125 - v1 public
```

show sys commands

The **`show sys`** commands display current system status and configuration.

show sys community command

The **`show sys community`** command displays the community strings on the switch.

Figure 40 shows output from the **`show sys community`** command.

Figure 40 show sys community command output

```
community :
                ro - public
                l1 - private
                l2 - private
                l3 - private
                rw - private
               rwa - secret
```

show sys diag info command

The **show sys diag info** command shows whether the ARU monitor is enabled or disabled.

Figure 41 shows output for the **show sys diag info** command.

Figure 41 show sys diag info command output

```
Passport 1100# show sys diag info

Diag Info :

        aru-monitor       : disable
```

show sys info command

The **show sys info** command lists the general system settings and status.

Figure 42 shows partial output for the **show sys info** command.

Figure 42 show sys info command output

```
Passport 1100# show sys info

General Info :

        SysName      : Passport 1100
        SysUpTime    : 42 day(s), 21:33:34
        SysContact   : support@baynetworks.com
        SysLocation  : 4401 Great America Parkway, Santa Clara, CA 95052

Chassis Info :

        Chassis : 1100
        Serial# : 60252
        HwRev   : v3.0
        NumSlots: 3
        AruMode : AruThree
        EocMode : default

Power Supply Info :

        Ps#1 Status       : up
        Ps#1 Type         : 110V AC Power Supply
        Ps#1 Serial Number:
        Ps#1 Version      :
--More-- (q = quit)
```

show sys perf command

The **show sys perf** command lists system performance information, such as:

- CPU utilization
- Switch Fabric utilization
- NVRAM size
- NVRAM used

This information is updated once per second. It is no more than one second from real time.

Figure 43 shows output for the **show sys perf** command.

Figure 43 show sys perf command output

```
            CpuUtil: 100%
  SwitchFabricUtil: 0%
        BufferUtil: 0%
         NVRamSize: 58 K
         NVRamUsed: 14 K
          DramSize: 32 M
          DramUsed: 54 %
          DramFree: 14883 K
```

show sys sw command

The command lists the version of software running on the Passport switch and the versions stored on the flash module and PCMCIA card, if applicable.

Figure 44 shows output for the **show sys sw** command.

Figure 44 show sys sw command output

```
Details        : rel2.1-new/current/main/hw/acc.st on Thu Feb 17 16:56:26 PST 20
00
LastBootSource : flash:3
Boot Monitor   : v2.1.0.b1
Runtime Config : flash:2
Device: flash
FN Name                              Flags    Length
-- ----                              -----    ------
1  syslog                              LN    131072
2  dana.cfg                            SN     14161
3  acc21newb15                        XZN   2024843
--                                            ------
3   files                      bytes used=   2228224 free=1966080
```

config sys link-flap-detect commands

Link flap detection allows you to set thresholds for the number and frequency of link state changes allowed on a physical port and to take action if the thresholds are exceeded. If the link state change thresholds are exceeded, a log entry is generated. The possible configuration actions: send a trap, and being down a port.

This feature allows you to detect when the link is going up and down rapidly (flapping) on a port. This action can be detrimental to network stability because it can trigger spanning and routing table recalculation.

config sys link-flap-detect followed by:	
auto-port-down <*enable*|*disable*>	Enables or disables the auto-port-down function.
frequency <*frequency*>	Sets the link-flap-detect frequency. • <*frequency*> is from 1 to 9999.
info	Shows the link-flap-detect settings.
interval <*interval*>	Sets the link-flap-detect interval. • <*intervals*> is from 2 to 600.
send-trap <*enable*|*disable*>	Enables or disables the send-trap function.

Figure 45 config sys link-flap-detect info command output

```
Passport 1100# config link-flap-detect info
config "link-flap-detect" not found
Passport 1100# config sys link-flap-detect info

 Auto Port Down : enable
 Send Trap      : enable
 Interval       : 60
 Frequency      : 10
```

Syslog commands

The syslog commands control the syslog, a feature in a UNIX machine that logs messages and assigns severities to the messages based on significance.

config sys syslog commands

The **`config sys syslog`** commands configure the syslog. Most of these commands require the host ID parameter for a UNIX host (1 to 10).

The **`config sys syslog`** commands use the following options:

`config sys syslog` followed by:	
`info`	Displays current syslog settings (Figure 46).
`host <id> address <ipaddr>`	Configures a host location for the syslog host, where `address` is the UNIX system syslog host IP address.
`host <id> create`	Creates a syslog host.
`host <id> delete`	Deletes a syslog host.
`host <id> facility <facility>`	Specifies the UNIX facility used in messages to the syslog host, where facility is the UNIX system syslog host facility (LOCAL0 to LOCAL7).
`host <id> <enable|disable>`	Enables or disables the syslog host.
`host <id>` info	Displays system log information for the specified host. This command results in the same output as the `show sys syslog host <id>` info command.

config sys syslog followed by:	
host <*id*> mapinfo <*level*>	Specifies the syslog severity level to use for Passport Information messages {emergency|alert|critical|error|warning|notice|info debug}.
host <*id*> mapwarning <*level*>	Specifies the syslog severity to use for Passport Warning messages {emergency|alert|critical|error|warning|notice|info|debug}.
host <*id*> maperror <*level*	Specifies the syslog severity to use for Passport Error messages {emergency|alert|critical|error|warning|notice|info|debug}.
host <*id*> mapfatal <*level*>	Specifies the syslog severity to use for Passport Fatal messages {emergency|alert|critical|error|warning|notice|info|debug}.
host <*id*> severity <*info*| *warning*|*error*|*fatal*> [<*info*|*warning*|*error*|*fatal*>]	Specifies the severity levels for which syslog messages should be sent for the specified modules, where severity is the severity for which syslog messages will be sent.
host <*id*> udp-port <*port*>	Specifies the UDP port number on which to send syslog messages to the syslog host, where udp-port is the UNIX system syslog host port number (514 to 530).
max-hosts <*maxhost*>	Specifies the maximum number of syslog hosts supported.
state<*enable*|*disable*>	Enables or disables sending syslog messages on the switch.

Figure 46 config sys syslog command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                    max-host : 5
                       state : enable
```

show commands

The **show** commands display information about the syslog feature as set up on the switch.

show sys syslog general info command

The **show sys syslog general info** command displays general information about the system log.

Figure 47 shows output for the **show sys syslog general info** command.

Figure 47 show sys syslog general info command output

```
Enable    : true
Max Hosts : 5
OperState : empty host table
Total number of configured hosts : 0
Total number of enabled hosts : 0
Configured host :
Enabled host :
```

show sys syslog host info command

The **show sys syslog host info** command displays system log information for the indicated host.

The command syntax is:

```
show sys syslog host <id> info
```

web-server commands

The **web-server** commands control the Passport Web interface.

config web-server commands

The **config web-server** commands allow you to enable, disable, and set passwords for the Passport Web interface. The commands use the following options:

Table 47-1.

config web-server followed by:	
info	Indicates if Web access is enabled or disabled.
disable	Turns off the Passport Web interface.
enable	Turns on the Passport Web interface.
set info	Displays the current Web user name and password setting.
set password <*ro*|*rw*|*rwa*> <*username*> <*passwd*>	Sets Web passwords where: <username> is the login name of the user. <passwd> is the password associated with the login name.

show web-server command

The **show web-server** command displays whether Web access is enabled. It also displays password and access information.

Figure 48 shows output for the **show web-server** command.

Figure 48 show web-server command output

```
Web Server Info :

        Status          : on
        RO Username     : ro
        RO Password     : ro
        RW Username     : rw
        RW Password     : rw
        RWA Username    : rwa
        RWA Password    : rwa
        NumHits         : 20
        NumAccessChecks: 0
        NumAccessBlocks: 0
        NumRxErrors     : 0
        NumTxErrors     : 2
        NumSetRequest   : 0
```

Chapter 5
Configuring layer 2 features

This chapter describes the CLI commands that are used to configure layer 2 (switching) functions in a Passport 1000 Series switch. The following sections are discussed:

- "Port commands," next
- "RADIUS commands" on page 142
- "Port Mirroring commands" on page 144
- "MLT commands" on page 146
- "Spanning tree group commands" on page 149
- "VLAN commands" on page 157

Port commands

Port commands manage the switch at the port level. This section includes the layer 2 port configuration and display commands. Port commands relating to layer 3 (routing) are covered in the following chapters, along with the related feature.

config ethernet ports commands

The **`config ethernet ports`** commands allow you to set layer 2 parameters for the specified ports on the switch. In all port commands, *`ports`* is the port or list of ports on which you are running the command.

The command syntax is:

```
{slot/port[-slot/port][, ...]}
```

These commands include media-layer commands and network-layer commands for the specified ports. The commands use the following options:

config ethernet <ports> followed by:	
`info`	Displays the current port settings (Figure 49).
`auto-negotiate <enable|disable>`	Enables or disables autonegotiation (adjusting between 10 Mb/s and 100 Mb/s and half- or full-duplex) on the port. See note on page 129. Enabled by default.
`duplex <half|full>`	Sets the operating mode of the port to half-duplex or full-duplex when autonegotiation is disabled.
`speed <10|100>`	Sets the port speed to 10 Mb/s or 100 Mb/s when autonegotiation is disabled.
`state <enable|disable|test>`	Specifies the administrative state on the port as up, down, or test. The default is up (enabled).
`default-vlan-id <vid>`	Directs the switch to send the untagged frames to a default VLAN if received on a tagged port. *vid* is the VLAN ID of the default VLAN to which the discarded frames should be sent.
`high-priority <true|false>`	Enables or disables setting the port as high priority.
`linktrap <enable|disable>`	Enables or disables the link up/down trap for a port.
`lock <true|false>`	Locks a port for exclusive use if the portlock feature is globally enabled with the command **`config sys set portlock on|off`**.
`name <name>`	Configures a port name.
`oversize-frame <enable|disable>`	Enables or disables large frame support.
`preferred-phy <left|right>`	Sets one of the two physical connectors (left or right) on a redundant port to be the primary connector. This command applies only to redundant Gigabit Ethernet ports.
`perform-tagging <enable|disable>`	Enables or disables the IEEE 802.1Q tagging on the port.
`tagged-frames-discard <enable|disable>`	Sets a port with tagging disabled to discard tagged frames. The default is disable.
`untagged-frames-discard <enable|disable>`	Sets a port with tagging enabled to discard untagged frames. The default is disable.
`unknown-mac-discard <enable|disable>`	Enables or disables if the port should discard unknown source MAC frames.

Note: The 10/100BASE-TX ports may not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, the settings can be manually configured for a link. Check the Nortel Networks Web site (nortelnetworks.com) for the latest compatibility information.

Figure 49 config ethernet info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

Port 1/1 :
                        lock : true
               auto-negotiate : true
                      duplex : half
               high-priority : false
                       speed : 10
         unknown-mac-discard : disable
              oversize-frame : disable
            default-vlan-id : 1
       tagged-frames-discard : disable
             perform-tagging : disable
     untagged-frames-discard : disable
                       state : up
                    linktrap : enable
```

show ports commands

The **`show ports`** commands display information about the switching setup, operation, and counters for all or specific ports. Definitions for the displayed fields are in Reference for Passport Management Software Switching Operations. The show ports commands relating to routing operation are listed in Chapter 6, "Configuring layer 3 protocol features."

The following command topics are included in this section:

- "show ports error collision command," next
- "show ports error main command" on page 131
- "show ports error extended command" on page 132
- "show ports info config command" on page 133
- "show ports info interface command" on page 134

- "show ports stats bridging command" on page 135
- "show ports stats interface main command" on page 136
- "show ports stats interface extended command" on page 137

show ports error collision command

The **show ports error collision** command displays the number and type of Ethernet collision errors for all or specified ports. Figure 50 on page 131 is a sample display.

The command syntax is:

```
show ports error collision [<ports>]
```

Figure 50 show ports error collision command output

```
================================================================================
                                    Port Ethernet Collision Error
================================================================================
PORT  -----------------COLLISIONS------------
NUM   SINGLE   MULTIPLE LATE     EXCESSIVE
--------------------------------------------------------------------------------
1/1   386      257      0        1
1/2   0        0        0        0
1/3   0        0        0        0
1/4   0        0        0        0
1/5   0        0        0        0
1/6   0        0        0        0
1/7   0        0        0        0
1/8   0        0        0        0
1/9   0        0        0        0
1/10  0        0        0        0
1/11  0        0        0        0
1/12  0        0        0        0
1/13  0        0        0        0
1/14  0        0        0        0
1/15  0        0        0        0
1/16  0        0        0        0
2/1   0        0        0        0
2/2   0        0        0        0
2/3   0        0        0        0
2/4   0        0        0        0
2/5   0        0        0        0
2/6   0        0        0        0
2/7   0        0        0        0
2/8   0        0        0        0
2/9   0        0        0        0
2/10  0        0        0        0
2/11  0        0        0        0
2/12  0        0        0        0
2/13  0        0        0        0
2/14  0        0        0        0
2/15  0        0        0        0
2/16  0        0        0        0
```

show ports error main command

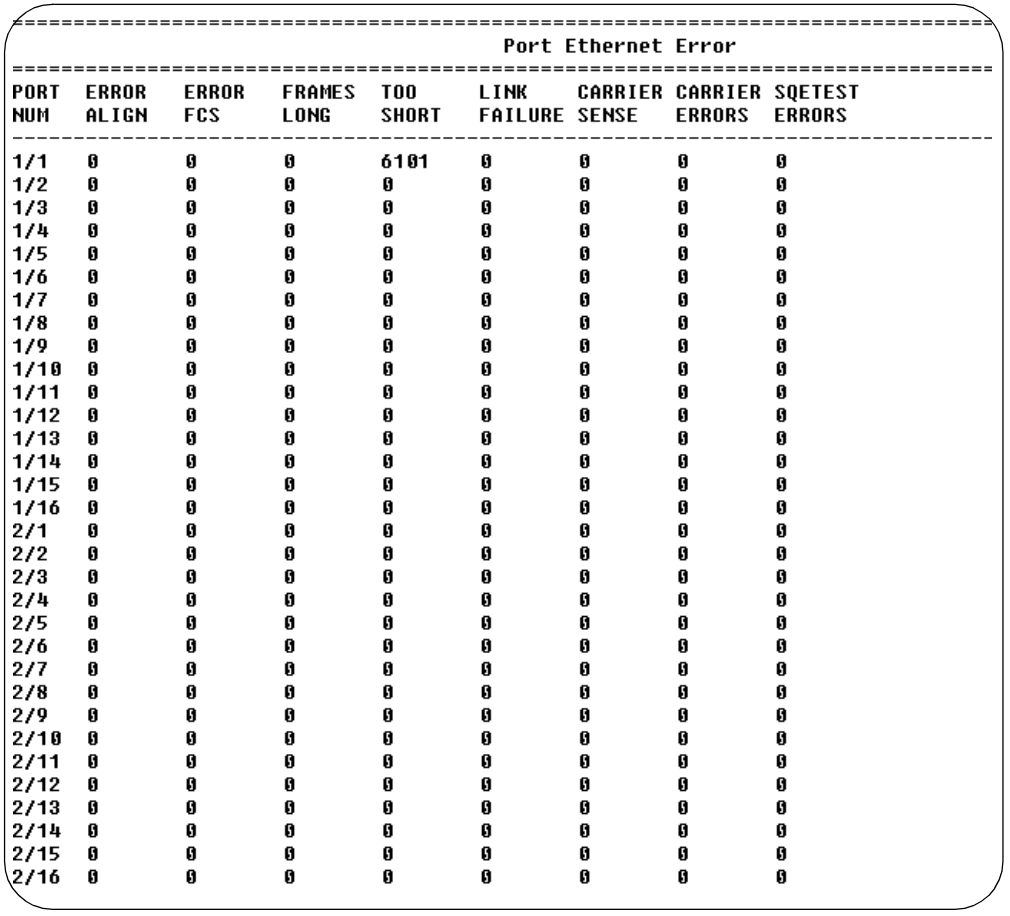
The **show ports error main** command displays information about the number of different types of Ethernet errors for all or specified ports.

The command syntax is:

```
show ports error main [<ports>]
```

Figure 51 shows output for the **show ports error main** command.

Figure 51 show ports error main command output



Port Ethernet Error

PORT NUM	ERROR ALIGN	ERROR FCS	FRAMES LONG	TOO SHORT	LINK FAILURE	CARRIER SENSE	CARRIER ERRORS	SQETEST ERRORS
1/1	0	0	0	6101	0	0	0	0
1/2	0	0	0	0	0	0	0	0
1/3	0	0	0	0	0	0	0	0
1/4	0	0	0	0	0	0	0	0
1/5	0	0	0	0	0	0	0	0
1/6	0	0	0	0	0	0	0	0
1/7	0	0	0	0	0	0	0	0
1/8	0	0	0	0	0	0	0	0
1/9	0	0	0	0	0	0	0	0
1/10	0	0	0	0	0	0	0	0
1/11	0	0	0	0	0	0	0	0
1/12	0	0	0	0	0	0	0	0
1/13	0	0	0	0	0	0	0	0
1/14	0	0	0	0	0	0	0	0
1/15	0	0	0	0	0	0	0	0
1/16	0	0	0	0	0	0	0	0
2/1	0	0	0	0	0	0	0	0
2/2	0	0	0	0	0	0	0	0
2/3	0	0	0	0	0	0	0	0
2/4	0	0	0	0	0	0	0	0
2/5	0	0	0	0	0	0	0	0
2/6	0	0	0	0	0	0	0	0
2/7	0	0	0	0	0	0	0	0
2/8	0	0	0	0	0	0	0	0
2/9	0	0	0	0	0	0	0	0
2/10	0	0	0	0	0	0	0	0
2/11	0	0	0	0	0	0	0	0
2/12	0	0	0	0	0	0	0	0
2/13	0	0	0	0	0	0	0	0
2/14	0	0	0	0	0	0	0	0
2/15	0	0	0	0	0	0	0	0
2/16	0	0	0	0	0	0	0	0

show ports error extended command

The **`show ports error extended`** command displays extended information about Ethernet errors for all or specified ports.

The command syntax is:

`show ports error extended [<`*`ports`*`>]`

Figure 52 shows output for the **`show ports error extended`** command.

Figure 52 show ports error extended command output

```
================================================================================
                                    Port Ethernet Error Extended
================================================================================
PORT  MAC_RX  MAC_TX  DIFFER  PACKET  LINK    UNKNOWN IN      OUT
NUM   ERRORS  ERRORS  TX      ERRORS  INACTIV PROTOS  FLWCTRL FLWCTRL
--------------------------------------------------------------------------------
1/1   0       0       577     0       0       0       0       0
1/2   0       0       0       0       0       0       0       0
1/3   0       0       0       0       0       0       0       0
1/4   0       0       0       0       0       0       0       0
1/5   0       0       0       0       0       0       0       0
1/6   0       0       0       0       0       0       0       0
1/7   0       0       0       0       0       0       0       0
1/8   0       0       0       0       0       0       0       0
1/9   0       0       0       0       0       0       0       0
1/10  0       0       0       0       0       0       0       0
1/11  0       0       0       0       0       0       0       0
1/12  0       0       0       0       0       0       0       0
1/13  0       0       0       0       0       0       0       0
1/14  0       0       0       0       0       0       0       0
1/15  0       0       0       0       0       0       0       0
1/16  0       0       0       0       0       0       0       0
2/1   0       0       0       0       0       0       0       0
2/2   0       0       0       0       0       0       0       0
2/3   0       0       0       0       0       0       0       0
2/4   0       0       0       0       0       0       0       0
2/5   0       0       0       0       0       0       0       0
2/6   0       0       0       0       0       0       0       0
2/7   0       0       0       0       0       0       0       0
2/8   0       0       0       0       0       0       0       0
2/9   0       0       0       0       0       0       0       0
2/10  0       0       0       0       0       0       0       0
2/11  0       0       0       0       0       0       0       0
2/12  0       0       0       0       0       0       0       0
2/13  0       0       0       0       0       0       0       0
2/14  0       0       0       0       0       0       0       0
2/15  0       0       0       0       0       0       0       0
2/16  0       0       0       0       0       0       0       0
```

show ports info config command

The **show ports info config** command displays general configuration information about all or specified ports.

The command syntax is:

```
ports info config [<ports>]
```

This information is also displayed when using the **show ports info all [<ports>]** command.

Figure 53 shows output for the **show ports info config** command.

Figure 53 show ports info config command output

```
================================================================================
                                    Port Config
================================================================================
PORT  LINK AUTO  ADMIN       OPERATE     HIGH     MLT PORT   OVERSZ DUAL
NUM   TRAP NEG.  DUPLX SPEED DUPLX SPEED PRIORITY ID  LOCKED FRAME  CONNECTOR
--------------------------------------------------------------------------------
1/1   true true  half  10    half  10    false    0   true   false
1/2   true true  half  10          0     false    0   false  false
1/3   true true  half  10          0     false    0   false  false
1/4   true true  half  10          0     false    0   false  false
1/5   true true  half  10          0     false    0   false  false
1/6   true true  half  10          0     false    0   false  false
1/7   true true  half  10          0     false    0   false  false
1/8   true true  half  10          0     false    0   false  false
1/9   true true  half  10          0     false    0   false  false
1/10  true true  half  10          0     false    0   false  false
1/11  true true  half  10          0     false    0   false  false
1/12  true true  half  10          0     false    0   false  false
1/13  true true  half  10    full  100   false    0   false  false
1/14  true true  half  10          0     false    0   false  false
1/15  true true  half  10          0     false    0   false  false
1/16  true true  half  10    full  100   false    0   false  false
2/1   true true  half  10    full  100   false    0   false  false
2/2   true true  half  10    full  100   false    0   false  false
2/3   true true  half  10          0     false    0   false  false
2/4   true true  half  10          0     false    0   false  false
2/5   true true  half  10          0     false    0   false  false
2/6   true true  half  10          0     false    0   false  false
2/7   true true  half  10          0     false    0   false  false
2/8   true true  half  10          0     false    0   false  false
2/9   true true  half  10          0     false    0   false  false
2/10  true true  half  10          0     false    0   false  false
2/11  true true  half  10          0     false    0   false  false
2/12  true true  half  10          0     false    0   false  false
2/13  true true  half  10          0     false    0   false  false
2/14  true true  half  10          0     false    0   false  false
2/15  true N/A   full  100         0     false    0   false  false
2/16  true N/A   full  100         0     false    0   false  false
```

show ports info interface command

The **show ports info interface** command displays information about the physical interface for all or specified ports.

The command syntax is:

```
show ports info interface [<ports>]
```

Figure 54 shows output for the **show ports info interface** command.

Figure 54 show ports info interface command output

```
================================================================================
                                  Port Interface
================================================================================
PORT                                          PHYSICAL          STATUS
NUM   INDEX DESCRIPTION    TYPE           MTU  ADDRESS           ADMIN  OPERATE
--------------------------------------------------------------------------------
1/1   16    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:00 up     up
1/2   17    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:01 up     down
1/3   18    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:02 up     down
1/4   19    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:03 up     down
1/5   20    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:04 up     down
1/6   21    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:05 up     down
1/7   22    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:06 up     down
1/8   23    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:07 up     down
1/9   24    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:08 up     down
1/10  25    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:09 up     down
1/11  26    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:0a up     down
1/12  27    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:0b up     down
1/13  28    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:0c up     up
1/14  29    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:0d up     down
1/15  30    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:0e up     down
1/16  31    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:0f up     up
2/1   32    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:10 up     up
2/2   33    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:11 up     up
2/3   34    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:12 up     down
2/4   35    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:13 up     down
2/5   36    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:14 up     down
2/6   37    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:15 up     down
2/7   38    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:16 up     down
2/8   39    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:17 up     down
2/9   40    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:18 up     down
2/10  41    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:19 up     down
2/11  42    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:1a up     down
2/12  43    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:1b up     down
2/13  44    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:1c up     down
2/14  45    100BaseTX     ethernetCsmacd 1500 00:e0:16:57:7e:1d up     down
2/15  46    100BaseF      ethernetCsmacd 1500 00:e0:16:57:7e:1e up     down
2/16  47    100BaseF      ethernetCsmacd 1500 00:e0:16:57:7e:1f up     down
```

show ports stats bridging command

The **show ports stats bridging** command displays port bridging information about all or specified ports.

The command syntax is:

```
show ports stats bridging [<ports>]
```

Figure 55 shows output for the **show ports stats bridging** command.

Figure 55 show ports stats bridging command output

```
================================================================================
                                  Port Stats Bridge
================================================================================
PORT     IN_FRAME   IN_FRAME   IN_FRAME   OUT_FRAME  OUT_FRAME  OUT_FRAME
NUM      UNICAST    MULTICAST  BROADCAST  UNICAST    MULTICAST  BROADCAST
--------------------------------------------------------------------------------
1/1      5614236    22725084   9740952    49763      1616877    0
1/2      0          0          0          0          0          0
1/3      0          0          0          0          0          0
1/4      0          0          0          0          0          0
1/5      0          0          0          0          0          0
1/6      0          0          0          0          0          0
1/7      0          0          0          0          0          0
1/8      0          0          0          0          0          0
1/9      0          0          0          0          0          0
1/10     0          0          0          0          0          0
1/11     0          0          0          0          0          0
1/12     0          0          0          0          0          0
1/13     0          3717689    0          0          3349704    0
1/14     0          0          0          0          0          0
1/15     0          0          0          0          0          0
1/16     0          1607107    0          0          4741895    0
2/1      1          3944948    218719     0          1962092    0
2/2      4          6551639    126        2956       2077915    0
2/3      0          0          0          0          0          0
2/4      0          0          0          0          0          0
2/5      0          0          0          0          0          0
2/6      0          0          0          0          0          0
2/7      0          0          0          0          0          0
2/8      0          0          0          0          0          0
2/9      0          0          0          0          0          0
2/10     0          0          0          0          0          0
2/11     0          0          0          0          0          0
2/12     0          0          0          0          0          0
2/13     0          0          0          0          0          0
2/14     0          0          0          0          0          0
2/15     0          0          0          0          0          0
2/16     0          0          0          0          0          0
```

show ports stats interface main command

The **show ports stats interface main** command displays basic interface information about all or specified ports.

The command syntax is:

```
show ports stats interface main [<ports>]
```

Figure 56 shows output for the **show ports stats interface main** command.

Figure 56 show ports stats interface main command output

```
================================================================================
                                    Port Stats Interface
================================================================================
PORT_NUM IN_OCTETS  OUT_OCTETS IN_PACKET  OUT_PACKET IN_FLOWCTRL   OUT_FLOWCTRL
--------------------------------------------------------------------------------
1/1      2615731078 118937702  38134348   1666737    0             0
1/2      0          0          0          0          0             0
1/3      0          0          0          0          0             0
1/4      0          0          0          0          0             0
1/5      0          0          0          0          0             0
1/6      0          0          0          0          0             0
1/7      0          0          0          0          0             0
1/8      0          0          0          0          0             0
1/9      0          0          0          0          0             0
1/10     0          0          0          0          0             0
1/11     0          0          0          0          0             0
1/12     0          0          0          0          0             0
1/13     237939520  214383356  3717805    3349734    0             0
1/14     0          0          0          0          0             0
1/15     0          0          0          0          0             0
1/16     102856896  309056284  1607139    4741983    0             0
2/1      119951437058 201850608  113319541  2798337    0             0

2/2      512593388  118237069999 7502956    108566166  0             0

2/3      0          0          0          0          0             0
2/4      0          0          0          0          0             0
2/5      0          0          0          0          0             0
2/6      0          0          0          0          0             0
2/7      0          0          0          0          0             0
2/8      0          0          0          0          0             0
2/9      0          0          0          0          0             0
2/10     0          0          0          0          0             0
2/11     0          0          0          0          0             0
2/12     0          0          0          0          0             0
2/13     0          0          0          0          0             0
2/14     0          0          0          0          0             0
2/15     0          0          0          0          0             0
2/16     0          0          0          0          0             0
```

show ports stats interface extended command

The **show ports stats interface extended** command displays extended port interface information for all or specified ports.

The command uses the syntax:

```
show ports stats interface extended [<ports>]
```

Figure 57 shows output for the **show ports stats interface extended** command.

Figure 57 show ports stats interface extended command output

```
================================================================================
                                  Port Stats Interface Extended
================================================================================
PORT_NUM IN_UNICST  OUT_UNICST IN_MULTICST  OUT_MULTICST IN_BRDCST  OUT_BRDCST
--------------------------------------------------------------------------------
1/1      5668210    49882      22725974     1616976      9741653    0
1/2      0          0          0            0            0          0
1/3      0          0          0            0            0          0
1/4      0          0          0            0            0          0
1/5      0          0          0            0            0          0
1/6      0          0          0            0            0          0
1/7      0          0          0            0            0          0
1/8      0          0          0            0            0          0
1/9      0          0          0            0            0          0
1/10     0          0          0            0            0          0
1/11     0          0          0            0            0          0
1/12     0          0          0            0            0          0
1/13     0          0          3717970      3349776      0          0
1/14     0          0          0            0            0          0
1/15     0          0          0            0            0          0
1/16     0          0          1607187      4742109      0          0
2/1      1          0          113101101    2798404      218740     0
2/2      104047     2956       7398989      108563544    126        0
2/3      0          0          0            0            0          0
2/4      0          0          0            0            0          0
2/5      0          0          0            0            0          0
2/6      0          0          0            0            0          0
2/7      0          0          0            0            0          0
2/8      0          0          0            0            0          0
2/9      0          0          0            0            0          0
2/10     0          0          0            0            0          0
2/11     0          0          0            0            0          0
2/12     0          0          0            0            0          0
2/13     0          0          0            0            0          0
2/14     0          0          0            0            0          0
2/15     0          0          0            0            0          0
2/16     0          0          0            0            0          0
```

show ports info vlans command

The **show ports info vlans** command displays VLAN information for all or specified ports.

The command syntax is:

```
show ports info vlans [<ports>]
```

Figure 58 shows output for the **show ports info vlans** command.

Figure 58 show ports info vlans command output

```
================================================================================
                                    Port Vlans
================================================================================
PORT          DISCARD DISCARD   DEFAULT VLAN
NUM   TAGGING TAGFRAM UNTAGFRAM VLANID  IDS
--------------------------------------------------------------------------------
1/1   disable false   false     1       1
1/2   disable false   false     1       0
1/3   disable false   false     1       0
1/4   disable false   false     1       0
1/5   disable false   false     1       0
1/6   disable false   false     1       0
1/7   disable false   false     1       0
1/8   disable false   false     1       0
1/9   disable false   false     1       0
1/10  disable false   false     1       237
1/11  disable false   false     1       0
1/12  disable false   false     1       0
1/13  disable false   false     1       0
1/14  disable false   false     1       0
1/15  disable false   false     1       0
1/16  disable false   false     1       0
2/3   disable false   false     1       0
2/4   disable false   false     1       0
2/5   disable false   false     1       0
2/6   disable false   false     1       0
2/7   disable false   false     1       0
2/8   disable false   false     1       0
2/9   disable false   false     1       0
2/10  disable false   false     1       0
2/11  disable false   false     1       3
2/12  disable false   false     1       3
2/13  disable false   false     1       0
2/14  disable false   false     1       0
2/15  disable false   false     1       0
2/16  disable false   false     1       0
```

config ethernet ports ip commands

The **config ethernet ports ip** commands allow you to assign and delete an IP address for a port.

config ethernet <ports> ip followed by:	
create <*ipaddr/mask*>	Creates an IP address and subnet mask to assign to the port {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. The mask can be expressed in dotted-decimal notation or as a number of bits.
delete <*ipaddr*>	Deletes the IP address assigned to the port (for example, 10.10.20.100).

config ethernet <ports> unknown-mac-discard commands

The **config ethernet <*ports*> unknown-mac-discard** commands configure the Unknown MAC Discard feature.

config ethernet <*ports*> unknown-mac-discard followed by:	
activation <*enable*|*disable*>	Enables the Unknown MAC Discard feature. Although you can configure the feature with it disabled, the Unknown MAC Discard feature *must* be enabled to be implemented.
add-allow-mac <*mac*> <*none*|*monitor*> <*low*|*high*>	Manually enters a MAC address into the allowed MAC table. Sets monitor and priority for specified MAC address (see below in table for explanations of monitor and priority).
autolearn <*enable*|*disable*>	Enables the autolearn mode on the port for populating the allowed MAC table. Autolearn does not take effect until Unknown MAC Discard is activated (see activation command above).
autolearn-mode <*one-shot*|*continuous*>	Sets the autolearn mode on the port for populating the allowed MAC table to: • one-shot • continuous

config ethernet <*ports*> unknown-mac-discard followed by:	
default-autolearn-monitor <*none*|*monitor*>	Sets the default field for the AutoLearn MAC. The options are: • none • monitor When “monitor” is selected, all MAC addresses are monitored if the port where the MAC addresses are learned is configured as a mirroring port. For more information, refer to Port Mirroring in the Accelar 2.0 documentation.
default-autolearn-priority <*low*|*high*>	Sets the priority of the traffic for the learned MAC address: • low • high
info	Displays the current configuration for the Unknown MAC Discard feature.
lock-autolearn-mac <*enable*|*disable*>	Enables the lock feature on the autolearn MAC’s address. When enabled, no new MAC addresses will be learned (one-shot or continuous); it sets the allowed MAC table to current state.
remove-allow-mac <*mac*>	Removes manually entered MAC address from allowed MAC table.
violation-downport <*enable*|*disable*>	Enables the selected port to automatically shut down when an intrusion occurs. To bring the port back up, the administrator must manually enable the selected port or reboot the system.
violation-logging <*enable*|*disable*>	Enables the system to create a system log entry when a disallowed MAC address attempts to send traffic through the selected port.
violation-sendtrap <*enable*|*disable*>	Enables the system to send an SNMP trap (rcMacViolation) when a frame from a disallowed MAC address is received.

The **show ports info** command displays port configuration for the Unknown MAC Discard feature.

show ports info followed by:	
unknown-mac-discard	Displays port configuration for the Unknown MAC Discard feature for the specified port.

RADIUS commands

The Passport 1000 Series chassis switch software supports Remote Authentication Dial-In User Service (RADIUS), which allows a remote RADIUS server, rather than the switch, to authenticate logins. The RADIUS server also provides access authority.

config radius commands

The **config radius** commands allow you to set up RADIUS authentication for the switch and include the following options:

config radius followed by:	
info	Displays the attribute value assigned, whether the RADIUS feature is enabled or disabled, and the maximum number of RADIUS servers.
attribute-value <*value*>	Sets the vendor-specific attribute to match the type value set in the dictionary file on the RADIUS server. Nortel Networks recommends always setting this field to 192 for the Passport 1000 Series chassis switches.
enable <true|false>	Enables or disables the RADIUS authentication feature.
maxserver <*value*>	Sets the maximum number of servers that you use. The *value* is between 1 and 10.

config radius followed by:	
server create <*ipaddr*> secret <*value*> [ports <*value*>] [priority <*value*>] [retry <*value*>] [timeout <*value*>] [enable <*value*>]	Creates and configures a server for the authentication feature: • *ipaddr*—the IP address of the server you want to add. • secret <*value*>—the secret key of the authentication client. • ports <*value*>—the UDP ports you want to use, from 1 to 65536. The default is 1812. • priority <*value*>—the priority, from 1 to 10, for this server. • retry <*value*>—the number of authentication retries the server will accept. • timeout <*value*>—the number of seconds before the authentication request times out. • enable <*value*>—to enable this server, set the value to true.
server set <*ipaddr*> [secret <*value*>] [ports <*value*>] [priority <*value*>] [retry <*value*>] [timeout <*value*>] [enable <*value*>]	Changes specified server values without having to delete the server and re-create it again. Configures a server for the authentication feature: • *ipaddr*—the IP address of the server you want to add. • secret <*value*>—the secret key of the authentication client**.** • ports <*value*>—the UDP ports you want to use, from 1 to 65536. The default is 1812. • priority <*value*>— the priority, from 1 to 10, for this server. • retry <*value*>— the number of authentication retries the server will accept. • timeout <*value*>— the number of seconds before the authentication request times out. • enable <*value*>—To enable this server, set the value to true.
server delete <*ipaddr*>	Deletes a server. Enter the IP address of the server you want to delete.
server info	Shows the RADIUS settings for the clients.

Note: The UDP port value set for the client must match the UDP port value set for the RADIUS server.

The **show radius** commands allow you to display the current settings for the RADIUS authentication feature. The **show radius** commands include the following options:

show radius followed by:	
info	Displays the current settings for the RADIUS server attribute value, operating status of the feature (enabled or not), and maximum number of servers allowed.
server config	Displays the current configuration settings for RADIUS servers.
server stat	Displays statistics for the RADIUS servers.

Port Mirroring commands

Port mirroring is a troubleshooting and network traffic analysis tool. Using port mirroring, you specify a destination port on which you want to see mirrored traffic and specify the source ports from which to mirror traffic. Any packet ingressing or egressing the specified ports is forwarded normally; a copy of the packet is sent out the mirror port. The Passport 1000 Series switch supports port mirroring on two ports. When this feature is active, all packets received on the ports specified as inport1 and/or inport2 are copied to the port specified as outport. The mirroring operation is nonintrusive.

Note: In ARU1 and ARU2 hardware, routed packets are not mirrored in the outgoing direction.

config mirror commands

The **config mirror** commands allow you to monitor one or two ports on a different port. The commands use the following options:

config mirror followed by:	
inport1 <*port*> <*enable*|*disable*>	Sets mirrored port 1 and enables or disables port mirroring on the port, where *port* is the slot/port in the format {slot/port[-slot/port][, ...]}.
inport2 <*port*> <*enable*|*disable*>	Sets mirrored port 2 and enables or disables port mirroring on the port, where *port* is the slot/port in the format {slot/port[-slot/port][, ...]}.
outport <*port*> <*enable*|*disable*>	Assigns and enables or disables the monitoring port, where *port* is the slot/port in the format {slot/port[-slot/port][, ...]}.
saveconfig <*true*|*false*>	Sets the switch to save or not save the mirror configuration information.

To monitor port 1/1 with output on port 1/16, the commands are:

```
Passport-1100# config mirror inport1 1/1 enable
Passport-1100# config mirror outport 1/16 enable
Passport-1100# config mirror saveconfig true
```

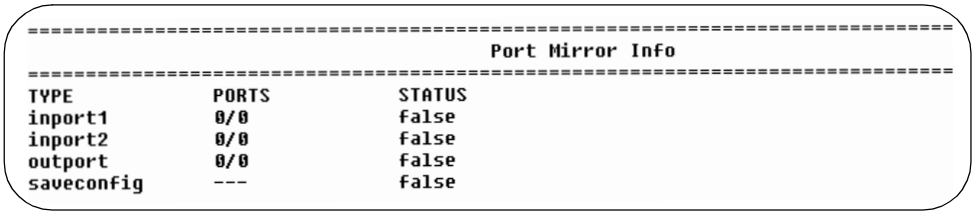
If using a network sniffer, connect the sniffer to port 1/16.

show mirrorinfo command

The **show mirrorinfo** command displays information about mirrored ports on the switch.

Figure 59 shows output for the **show mirrorinfo** command.

Figure 59 show mirrorinfo command output



```
================================================================================
                                  Port Mirror Info
================================================================================
TYPE            PORTS           STATUS
inport1         0/0             false
inport2         0/0             false
outport         0/0             false
saveconfig      ---             false
```

MLT commands

The MLT commands control MultiLink Trunking (MLT) on the switch. MLT is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth.

Note: Implementation of MLT requires hardware that is ARU2 or above (-A or -B modules or later).

config mlt commands

The **`config mlt`** commands set up MLT on the switch and have the parameter *`mid`* for the MLT ID (1 to 8) and the following options:

`config mlt <mid>` followed by:	
`info`	Displays current settings for the MLT (Figure 60).
`add info`	Displays ports and VLANs added to the MLT (Figure 61).
`remove info`	Displays the ports/VLANs removed from the MLT.
`add ports <`*`ports`*`>`	Adds ports to the MLT.
`add vlan <`*`vid`*`>`	Adds a VLAN to the MLT.
`create`	Creates an MLT.
`delete`	Deletes an MLT.
`name <`*`string`*`>`	Names an MLT.

config mlt <mid> followed by:	
remove ports <*ports*>	Removes ports from the MLT.
remove vlan <*vid*>	Removes a VLAN from the MLT.
perform tagging <*enable*|*disable*>	Sets the MLT as a tagged or nontagged port.

Figure 60 config mlt info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                      create : 1
                      delete : N/A
                        name : MLT-1
             perform-tagging : disable
```

Figure 61 config mlt add info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                       ports :
                        vlan :
```

show mlt commands

The **show mlt** commands are used to display information and statistics about MLT on the switch.

show mlt error collision command

The **show mlt error collision** command displays information about collision errors in a specified MultiLink Trunk or all MLTs.

The command syntax is:

```
show mlt error collision [<mid>]
```

Figure 62 shows output for the **show mlt error collision** command.

Figure 62 show mlt error collision command output

```
================================================================================
                                  Mlt Collision Error
================================================================================
MLT   -----------------COLLISIONS------------
ID    SINGLE   MULTIPLE LATE     EXCESSIVE
--------------------------------------------------------------------------------
1     0        0        0        0
```

show mlt error main command

The **show mlt error main** command displays information about the types of Ethernet errors sent and received by a specified MLT or all MLTs.

The command syntax is:

`show mlt error main [<mid>]`

IMAC refers to internal MAC address errors.

Figure 63 shows output for the **show mlt error main** command.

Figure 63 show mlt error main command output

```
================================================================================
                                  Mlt Ethernet Error
================================================================================
MLT  ALIGN   FCS     IMAC    IMAC    CARRIER FRAMES  SQETEST DEFER
ID   ERROR   ERROR   TRNSMIT RECEIVE SENSE   TOOLONG ERROR   TRNSMSS
--------------------------------------------------------------------------------
1    0       0       0       0       0       0       0       0
```

show mlt info command

The **show mlt info** command displays the status of MLT for the switch or the specified MLT ID.

The command syntax is:

`show mlt info [<mid>]`

Figure 64 shows the output for the **show mlt info** command.

Figure 64 show mlt info command output

```
================================================================================
                                    Mlt Info
================================================================================
                        PORT            PORT          VLAN
IFINDEX NAME            TYPE            MEMBERS       IDS
--------------------------------------------------------------------------------
1       MLT-1           access
```

show mlt stats command

The **`show mlt stats`** command displays MLT statistics for the switch or the specified MLT ID.

The command syntax is:

`show mlt stats [<mid>]`

Figure 65 shows output for the **`show mlt stats`** command.

Figure 65 show mlt stats command output

```
================================================================================
                                  Mlt Interface
================================================================================
MLT    IN       OUT      IN       OUT      IN       OUT      IN       OUT
ID     OCTETS   OCTETS   UNICST   UNICST   MULTICST MULTICST BROADCST BROADCST
--------------------------------------------------------------------------------
1      0        0        0        0        0        0        0        0
```

Spanning tree group commands

The **`spanning tree group`** commands configure parameters for a spanning tree group (STG) and for ports in that group. It also allows you to enable or disable the Spanning Tree Protocol in an STG.

config stg commands

The **config stg commands** configure parameters for the spanning tree group with the defined spanning tree group ID (<*sid*> is from 1 to 25).

The commands use the following options:

config stg <sid> followed by:	
info	Displays characteristics of a spanning tree group.
add-port <*ports*>	Adds ports to a spanning tree group.
create [<*ports*>] [mac <*value*>] [vlan <*value*>]	Creates a new spanning tree group.
delete	Deletes a spanning tree group.
forward-delay <*timeval*>	Sets the bridge forward delay time in 1/100 seconds (400 to 3000).
group-stp <*enable*|*disable*>	Enables or disables a spanning tree on a specified STG.
hello-interval <*timeval*>	Sets the bridge hello time in 1/100 seconds (400 to 3000).
max-age <*timeval*>	Sets the bridge maximum age time in 1/100 seconds (600 to 4000).
priority <*number*>	Sets bridge priority number (0 to 65535).
remove-ports <*value*>	Removes ports from a spanning tree group.
trap-stp <*enable*|*disable*>	Enables or disables the STG trap for a specific spanning tree group.

Note: Disabling spanning tree can slightly reduce CPU overhead. However, unless you are using the switch in a simple network with little possibility of having loops, Nortel Networks recommends that you leave spanning tree enabled.

Figure 66 shows output for the **config stg info** command.

Figure 66 config stg info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                  add ports : 1/1,1/9-1/12,1/14-1/15
                     create : 1
                     delete : N/A
              forward-delay : 1500
                  group-stp : true
             hello-interval : 200
                    max-age : 2000
                   priority : 32768
               remove ports : N/A
                   trap-stp : true
```

config ethernet ports stg commands

The **`config ethernet ports stg`** commands configure parameters for the ports in the specified spanning tree group.

The command syntax is:

`config ethernet <`*`ports`*`> stg <`*`sid`*`>`

where:

`ports` is the port, or list of ports, on which you are running the command {`slot/port[-slot/port][, ...]`}.

`sid` is the spanning tree group ID (1 to 25).

The commands use the following options:

config ethernet <ports> stg <sid> followed by:	
info	Displays current settings for the port spanning tree group.
faststart <*enable*|*disable*>	Enables or disables the FastStart feature. When FastStart is enabled, the port goes through the normal listening and learning states before forwarding. The hold time for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).
pathcost <*intval*>	Sets the contribution of this port to the path cost. *intval* is the cost {1 to 65535}.
priority <*intval*>	Sets the priority of this port. *intval* is the priority {0 to 255}.
stp <*enable*|*disable*>	Enables or disables the Spanning Tree Protocol.

Figure 67 shows output for the **config ethernet stg info** command.

Figure 67 config ethernet stg info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

Port 1/1 :
                    faststart : disable
                     pathcost : 100
                     priority : 128
                          stg : enable
```

show stg commands

The **show stg** commands display the status of a spanning tree on a switch or a port.

show stg info config command

The **show stg info config** command displays the spanning tree group configuration for the switch or for the specified spanning tree group.

The command uses the syntax:

```
show stg info config [<sid>]
```

Figure 68 shows output for the **show stg info config** command.

Figure 68 show stg info config command output

```
================================================================================
                                    Stg Config
================================================================================
STG           BRIDGE  BRIDGE     FORWARD ENABLE STPTRAP
ID   PRIORITY MAX_AGE HELLO_TIME DELAY   STP    TRAP
--------------------------------------------------------------------------------
1    32768    2000    200        1500    true   true
2    32768    2000    200        1500    true   true
4    32768    2000    200        1500    true   true
5    32768    2000    200        1500    true   false
20   32768    2000    200        1500    false  false
21   32768    2000    200        1500    true   true
22   32768    2000    200        1500    true   true

STG  TAGGBPDU           TAGGBPDU PORT
ID   ADDRESS            VLAN_ID MEMBER
--------------------------------------------------------------------------------
1    00:00:00:00:00:00  0       3/1-3/2,3/7-3/8,3/16
```

show stg info status command

The **show stg info status** command displays the spanning tree group status for a specified STG or all STGs.

The command uses the syntax:

```
show stg info status [<sid>]
```

Figure 69 shows output for the **show stg info status** command.

Figure 69 show stg info status command output

```
================================================================================
                                  Stg Status
================================================================================
STG  BRIDGE             NUM   PROTOCOL      TOP
ID   ADDRESS            PORTS SPECIFICATION CHANGES
--------------------------------------------------------------------------------
1    00:e0:16:83:26:01 5     ieee8021d     80
2    00:e0:16:83:26:02 4     ieee8021d     0
4    00:e0:16:83:26:04 1     ieee8021d     0
5    00:e0:16:83:26:05 2     ieee8021d     96
20   00:e0:16:83:26:14 2     ieee8021d     0
21   00:e0:16:83:26:15 0     ieee8021d     0
22   00:e0:16:83:26:16 0     ieee8021d     0

STG  DESIGNATED               ROOT  ROOT  MAX  HELLO  HOLD  FORWARD
ID   ROOT                     COST  PORT  AGE  TIME   TIME  DELAY
--------------------------------------------------------------------------------
1    80:00:00:00:00:a1:a2:a5 200   3/1   2000 200    100   1500
2    80:00:00:e0:16:83:26:02 0     cpp   2000 200    100   1500
4    80:00:00:e0:16:83:26:04 0     cpp   2000 200    100   1500
5    80:00:00:00:00:a1:a2:a5 220   3/10  2000 200    100   1500
20   00:00:00:00:00:00:00:00 0     cpp   2000 200    100   1500
```

show ports info stg main command

The **`show ports info stg main`** command displays STG information about a specified port or all ports.

The command syntax is:

`show ports info stg main [<`*`ports`*`>]`

Figure 70 shows output for the **`show ports info stg main`** command.

Figure 70 show ports info stg main command output

```
================================================================================
                                    Port Stg
================================================================================
PORT_NUM PRIORITY STATE      ENABLESTP FASTSTART PATHCOST FORWARD_TRANSITION
--------------------------------------------------------------------------------
3/1      128      forwarding true      false     100      1
3/2      128      disabled   true      false     100      0
3/3      128      disabled   true      false     100      0
3/4      128      disabled   true      false     100      0
3/5      128      disabled   true      false     100      0
3/6      128      disabled   true      false     100      0
3/7      128      disabled   true      false     100      0
3/8      128      disabled   true      false     100      0
3/9      128      blocking   true      false     10       0
3/10     128      forwarding true      false     10       1
3/11     128      disabled   true      false     100      0
3/12     128      disabled   true      false     100      0
3/14     128      disabled   true      false     100      0
3/16     128      disabled   true      false     100      0
```

show ports info stg extended command

The **show ports info stg extended** command displays extended STG information for all or a specified port.

The command uses the syntax:

```
show ports info stg main [<ports>]
```

Figure 71 shows output for the **show ports info stg extended** command.

Figure 71 show ports info stg extended command output

```
================================================================================
                                  Port Stg Extended
================================================================================

          ----------------------DESIGNATED----------------
PORT_NUM   ROOT                    COST       BRIDGE                   PORT
--------------------------------------------------------------------------------
3/1        80:00:00:00:00:a1:a2:a5 100        80:00:00:80:2d:39:f0:01 80:43
3/2        80:00:00:00:00:a1:a2:a5 200        80:00:00:e0:16:83:26:01 80:31
3/3        80:00:00:e0:16:83:26:02 0          80:00:00:e0:16:83:26:02 80:32
3/4        80:00:00:e0:16:83:26:02 0          80:00:00:e0:16:83:26:02 80:33
3/5        80:00:00:e0:16:83:26:02 0          80:00:00:e0:16:83:26:02 80:34
3/6        80:00:00:e0:16:83:26:02 0          80:00:00:e0:16:83:26:02 80:35
3/7        80:00:00:00:00:a1:a2:a5 200        80:00:00:e0:16:83:26:01 80:36
3/8        80:00:00:00:00:a1:a2:a5 200        80:00:00:e0:16:83:26:01 80:37
3/9        80:00:00:00:00:a1:a2:a5 210        80:00:00:e0:16:83:28:01 80:39
3/10       80:00:00:00:00:a1:a2:a5 210        80:00:00:e0:16:83:28:01 80:38
3/11       00:00:00:00:00:00:00:00 0          00:00:00:00:00:00:00:00 00:00
3/12       00:00:00:00:00:00:00:00 0          00:00:00:00:00:00:00:00 00:00
3/14       00:00:00:00:00:00:00:00 0          00:00:00:00:00:00:00:00 00:00
3/16       80:00:00:00:00:a1:a2:a5 200        80:00:00:e0:16:83:26:01 80:3f
```

show ports stats stg command

The **`show ports stats stg`** command displays counter information about STG on all or specified ports.

The command syntax is:

`show ports stats stg [<`*`ports`*`>]`

Figure 72 shows output for the **`show ports stats stg`** command.

Figure 72 show ports stats stg command output

```
================================================================================
                                  Port Stats Stg
================================================================================
PORT      IN_CONFIG  IN_TCU     IN_BAD     OUT_CONFIG OUT_TCU
NUM       BPDU       BPDU       BPDU       BPDU       BPDU
--------------------------------------------------------------------------------
3/1       365003     356        0          37         29
3/2       0          0          0          0          0
3/3       0          0          0          0          0
3/4       0          0          0          0          0
3/5       0          0          0          0          0
3/6       0          0          0          0          0
3/7       0          0          0          0          0
3/8       0          0          0          0          0
3/9       364660     16         0          162        5
3/10      364649     33         0          144        54
3/11      0          0          0          0          0
3/12      0          0          0          0          0
3/13      0          0          0          0          0
3/14      0          0          0          0          0
3/15      0          0          0          0          0
3/16      0          0          0          0          0
```

VLAN commands

The VLAN commands allow you to create VLANs, add VLANs to specific ports, set VLAN characteristics, and view VLAN information. VLAN commands that set VLAN routing parameters are discussed in Chapter 6, “Configuring layer 3 protocol features.”

config vlan create commands

The **`config vlan create`** commands are used to create a VLAN. You can create four types of VLANs using Passport software:

- Port VLANs
- Protocol VLANs
- IP subnet VLANs
- Source MAC address VLANs

The command syntax is:

```
<vid> is the VLAN ID (from 2 to 4095)
```

VLAN 1 is the default VLAN. The commands use the following options:.

config vlan <vid> create followed by:	
create byport <*sid*> [name<value>]	Creates a port-based VLAN, with spanning tree ID 1 to 25.The name *value* is the name of the VLAN {string}.
create byprotocol <*sid*> <*ip|ipx802dot3|ipx802dot2|ipxSnap|ipxEthernet2|appleTalk|decLat|decOther|sna802dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp*> [pid] [name<*value*>]	Creates a protocol-based VLAN with spanning tree ID 1 to 25. • pid is a user-defined protocol ID number in hex (0 to 65535). • name *value* is the name of the VLAN {string}.
create by ipsubnet <*sid*> <*ipaddr/mask*> [name <*value*>]	Creates an IP subnet-based VLAN with spanning tree ID 1 to 25. • *ipaddr/mask* is the IP address and mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • name *value* is the name of the VLAN {string.}
create bysrcmac <*sid*> [name <*value*>]	Creates a VLAN by source MAC address with spanning tree ID 1 to 25. name *value* is the name of the VLAN {string}.
create info	Displays information about the type of the specified VLAN.

Figure 73 shows output for the **config vlan create** command.

Figure 73 config vlan create info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                    byport :
                                sid - 1
                               name - Default
```

config vlan general commands

The **config vlan general** commands are used to:

- Add or remove ports in a VLAN
- Set priority
- Change a VLAN name

For all VLAN commands, *vid* is the VLAN ID (from 1 to 4095).

The generic VLAN commands use the following options:

config vlan <vid> followed by:	
info	Displays characteristics of the specified VLAN (Figure 74).
action <*action choice*>	Sets the VLAN action: {none| flushMacFdb |flushArp|flushIp|flushDynMemb |all| flushSnoopMemb|triggerRipUpdate|flushSnoop MRtr}.
agetime<10..100000>	Sets the VLAN aging time in seconds (10 to 1000000).
delete	Deletes a VLAN.
highpriority <*true*|*false*>	Configures the VLAN high-priority setting to on (true) or off (false).
name<*vname*>	Changes the name of a VLAN to <vname> {string} .
ports add <*ports*> [member<*value*>]	Adds ports to a VLAN. • *ports* is the port list {slot/port[-slot/port][,...]}. • member *value* is the port member type (portmember|static|notallowed) for always, sometimes, or never a member.
ports info	Displays member status of the ports in the VLAN (Figure 75).
ports remove <*ports*> [member <*value*>]	Removes ports from a VLAN but does not delete the VLAN.
srcmacadd <*macaddr*>	Adds a source MAC address to a VLAN. <*mac*> is the MAC address {0x00:0x00:0x00:0x00:0x00:0x00}.

config vlan <vid> followed by:	
`srcmac info`	Displays MAC addresses added to or removed from the VLAN (Figure 76).
`srcmac remove <macaddr>`	Removes the source MAC address from the VLAN. *mac* is the MAC address {0x00:0x00:0x00:0x00:0x00:0x00}.

Figure 74 config vlan info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                     action : N/A
                    agetime : N/A
                     delete : N/A
               highpriority : false
                       name : Default
```

Figure 75 config vlan ports info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                        add :
                           portmember - 3/1-3/2
                         activemember - 3/1-3/2
                         staticmember -
                       notallowtojoin -
                     remove : N/A
```

Figure 76 config vlan srcmac info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                        add :
                     remove : N/A
```

show vlan general commands

The show vlan general commands provide configuration information about all VLANs on the switch or specified VLANs.

show vlan info command

The **show vlan info** command displays entries for the MAC table.

show vlan info followed by:	
manual-edit-mac	Displays entries that are manually entered into the allowed MAC table.
autolearn-mac	Displays entries that are autolearned by the switch (one-shot or continuous) for the allowed MAC table.

show vlan info basic command

The **show vlan info basic** command displays the basic configuration for all or the specified VLAN.

The command uses the syntax:

```
show vlan info basic [<vid>]
```

Figure 77 shows output for the **show vlan info basic** command.

Figure 77 show vlan info basic command output

```
================================================================================
                                    Vlan Basic
================================================================================
VLAN                              STG
ID   NAME             TYPE        ID  PROTOCOLID SUBNETADDR      SUBNETMASK
--------------------------------------------------------------------------------
1    Default          byPort      1   none       N/A             N/A
2    VLAN-2           byIpSubnet  2   none       168.168.1.0     255.255.255.0
45   MM-16            byPort      4   none       N/A             N/A
75   ubs              byPort      5   none       N/A             N/A
76   vines            byProtocolId 1  vines      N/A             N/A
77   ipx802dot2       byProtocolId 1  ipx802dot2 N/A             N/A
78   brouter          byProtocolId 0  ip         N/A             N/A
```

show vlan info advance command

The **show vlan info advance** command shows parameters for all or specified VLANs.

The command syntax is:

```
show vlan info advance [<vid>]
```

Figure 78 shows output for the **show vlan info advance** command.

Figure 78 show vlan info advance command output

```
================================================================================
                                  Vlan Advance
================================================================================
VLAN        IF    HIGH     AGING MAC                              USER
ID  NAME    INDEX PRIORITY TIME  ADDRESS            ACTION RESULT  DEFINEPID
--------------------------------------------------------------------------------
1   Default 257   false    N/A   00:e0:16:83:26:81  none   none    0
2   VLAN-2  265   false    600   00:00:00:00:00:00  none   none    0
45  MM-16   259   false    N/A   00:e0:16:83:26:83  none   none    0
75  ubs     258   false    N/A   00:00:00:00:00:00  none   none    0
76  vines   263   false    600   00:00:00:00:00:00  none   none    0
77  ipx802dot2 264   false    600   00:00:00:00:00:00  none   none    0
78  brouter 260   false    600   00:00:00:00:00:00  none   success 0
```

show vlan info fdb-entry command

The **show vlan info fdb-entry** command displays forwarding database information for a specified VLAN.

The command syntax is:

```
show vlan info fdb-entry <vid>
```

Figure 79 shows output for the **show vlan info fdb-entry** command.

Figure 79 show vlan info fdb-entry command output

```
================================================================================
                                    Vlan Fdb
================================================================================
VLAN          MAC
ID   STATUS   ADDRESS            PORT MONITOR PRIORITY
--------------------------------------------------------------------------------
1    mgmt     00:00:79:01:02:03  3/1  false   low
1    learned  00:00:81:bc:ea:00  3/1  false   low
1    learned  00:00:81:bc:ea:81  3/1  false   low
1    learned  00:00:81:c1:9b:81  3/1  false   low
1    learned  00:00:81:c1:f6:81  3/1  false   low
1    learned  00:00:81:c4:da:23  3/1  false   low
1    learned  00:00:81:e1:4a:f5  3/1  false   low
1    learned  00:00:81:e1:4b:46  3/1  false   low
1    learned  00:08:c7:02:c4:c0  3/1  false   low
1    learned  00:60:5c:83:2f:08  3/1  false   low
1    learned  00:60:fd:91:22:d1  3/1  false   low
1    learned  00:60:fd:92:07:91  3/1  false   low
1    learned  00:60:fd:9e:2b:6b  3/1  false   low
1    learned  00:60:fd:bb:0e:c3  3/1  false   low
1    learned  00:60:fd:ee:19:b2  3/1  false   low
1    learned  00:80:2d:06:e5:39  3/1  false   low
```

show vlan info fdb-filter command

The **`show vlan info fdb-filter`** command displays the forwarding database filters for a specified VLAN.

The command syntax is:

`show vlan info fdb-filter <`*`vid`*`>`

The display includes:

- VLAN ID
- VLAN status
- VLAN MAC address
- Ports from which the VLAN is not allowed to receive frames

show vlan info fdb-static command

The **`show vlan info fdb-static`** command displays the static forwarding database status and priority for a specified VLAN.

The command syntax is:

```
show vlan info fbd-static <vid>
```

show vlan info ports command

The **show vlan info ports** command displays the port member status for all or a specified VLAN.

The command syntax is:

```
show vlan info ports [<vid>]
```

Figure 80 shows output for the **show vlan info ports** command.

Figure 80 show vlan info ports command output

```
================================================================================
                                  Vlan Advance
================================================================================
VLAN        IF    HIGH     AGING MAC                          USER
ID  NAME    INDEX PRIORITY TIME  ADDRESS           ACTION RESULT  DEFINEPID
--------------------------------------------------------------------------------
1   Default 257   false    N/A   00:e0:16:83:26:81  none   none    0
2   VLAN-2  265   false    600   00:00:00:00:00:00  none   none    0
45  MM-16   259   false    N/A   00:e0:16:83:26:83  none   none    0
75  ubs     258   false    N/A   00:00:00:00:00:00  none   none    0
76  vines   263   false    600   00:00:00:00:00:00  none   none    0
77  ipx802dot2 264   false    600   00:00:00:00:00:00  none   none    0
78  brouter 260   false    600   00:00:00:00:00:00  none   success 0
```

show vlan info srcmac command

The **show vlan info srcmac** command displays the source MAC address for any source MAC-based VLANs or for a specified VLAN if it is source MAC based.

Figure 81 shows output for the **show vlan info srcmac** command.

Figure 81 show vlan info srcmac command output

config vlan fdb (forwarding database) commands

The **config vlan fdb** (forwarding database) commands use the following options:

config vlan <vid> fdb followed by:	
-entry aging-time<*seconds*>	Sets the timeout period in seconds for the forwarding VLAN forwarding database (10 to 10000).
-entry flush	Flushes the entry from the forwarding database.
-entry info	Displays current characteristics of the forwarding database entry (Figure 82).
-entry monitor<*mac*> status <*value*> <*true*|*false*>	Sets the VLAN forwarding database monitor to on (true) or off (false). • <mac> is the MAC address {0x00: 0x00:0x00:0x00:0x00:0x00:0x00}. • status *value* is the forwarding database status {other| invalid|learned|self|mgmt}.
-entry priority<*mac*> status <*value*> <*high*|*low*>	Sets the VLAN forwarding database priority to high or low. • <mac> is the MAC address {0x00: 0x00:0x00:0x00:0x00:0x00:0x00}. • status *value* is the forwarding database status {other| invalid|learned|self|mgmt}.
-filter add <*mac*> port <*value*>	Adds a filter member to a VLAN bridge. • *mac* is the MAC address {0x00: 0x00:0x00:0x00:0x00:0x00:0x00}. • port *value* is the slot/port {slot/port[-slot/port][,...]}.
-filter info	Indicates forwarding database filters added or removed (Figure 83).

config vlan <vid> fdb followed by:	
-filter notallowfrom add <*mac*> port <*value*>	Adds a not-allowed filter member to a VLAN bridge. • *mac* is the MAC address {0x00:0x00:0x00:0x00:0x00:0x00}. • port *value* is the portlist {slot/port[-slot/port][,...]}.
-filter notallowfrom info	Displays not-allowed filter members added or removed (Figure 84).
-filternotallowfrom remove <*mac*> port <*value*>	Removes a not-allowed filter member from a VLAN bridge. • *mac* is the MAC address {0x00:0x00:0x00:0x00:0x00:0x00}. • port *value* is the portlist {slot/port[-slot/port][,...]}.
-filter remove <*mac*>	Removes a filter member from a VLAN bridge, where *mac* is the MAC address {0x00:0x00:0x00:0x00:0x00:0x00}.
-static add <*mac*> port <*value*>	Adds a static member to a VLAN bridge. • *mac* is the MAC address {0x00:0x00:0x00:0x00:0x00:0x00}. • port *value* is the slot/port {slot/port[-slot/port][,...]}.
-static info	Displays static members added or removed (Figure 85).
-static remove <*mac*>	Removes a static member from a VLAN, where *mac* is the MAC address {0x00:0x00:0x00:0x00:0x00:0x00}.

Figure 82 config vlan fdb-entry info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                  aging-time : 300
                       flush : N/A
                     monitor : false
                    priority : low
                                 mac - 00:00:79:01:02:03
                              status - mgmt

                     monitor : false
                    priority : low
                                 mac - 00:00:81:bc:ea:00
                              status - learned

                     monitor : false
                    priority : low
                                 mac - 00:00:81:bc:ea:81
                              status - learned

                     monitor : false
                    priority : low
                                 mac - 00:00:81:c1:9b:81
                              status - learned

                     monitor : false
                    priority : low
                                 mac - 00:00:81:c1:f6:81
                              status - learned
```

Figure 83 config vlan fdb-filter info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                          add :
                       remove : N/A
```

Figure 84 config vlan fdb filter notallowfrom info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                          add :
                       remove : N/A
```

Figure 85 config vlan fdb-static info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                          add :
                                    mac - 00:00:79:01:02:03
                                   port - 3/1
                       remove : N/A
```

config vlan igmp-snoop commands

The Internet Group Management Protocol (IGMP) is used by hosts to report multicast group memberships to neighbor multicast routers. IP multicasting provides services such as delivery of information to multiple destinations with a single transmission and the solicitation of servers by clients. The Passport switch supports IGMPv1 and IGMPv2 to prune group membership per port within a VLAN. This feature is called IGMP snooping.

Note: Implementation of IGMP snooping requires ARU2 or later hardware (-A and -B modules). Sender (source) and access functions require ARU3 (-B hardware). The switch functions in the mode of the lowest hardware present. If an -A module is installed in a switch and you attempt to use the sender or access commands, you receive an "Incompatible Hardware" message.

The IGMP snooping feature allows the user to optimize the multicast data flow for a group within a VLAN only to those that are members of the group. The switch listens to group reports from each port and builds a database of multicast group members per port. It suppresses the reports heard by not forwarding them to other hosts, forcing the members to continuously send their own reports. It multicasts data only to the participating group members and to the multicast routers within the VLAN.

The commands use the following options:

config vlan <vid> igmp-snoop followed by:	
`info`	Displays IGMP-snooping characteristics of the VLAN (Figure 86).
`access-list create <GroupAddress> <HostAddress> <HostMask> <denyRX|denyTX|denyBoth>`	Creates an access list to control access to IGMP group membership. • Group Address is the multicast group address of the multicast stream. • Host Address is the IP address of the host whose membership is being controlled. The options are to deny receive mode, deny transmit mode, or deny both.
`access-list delete <GroupAddress> <HostAddress> <HostMask>`	Deletes the access list controlling IGMP group membership.
`access-list <GroupAddress> info`	Displays the access list for the specified multicast address.
`access-list <GroupAddress> mode <HostMask> <denyRX|denyTX|denyBoth>`	Sets the mode for a group address host mask to deny receive mode, deny transmit mode, or deny both.
`mrouter <ports>`	Sets the ports directly and indirectly attached to a multicast router so the multicast data is forwarded to the router. These are static entries, not to be confused with dynamic entries, which are learned dynamically. <ports> is the port list {slot/port[-slot/port][,...]}.
`query-interval <seconds>`	Sets the query interval (in seconds), the time between queries sent to the host, and determines the multicast group membership timeouts. This should be the same value as that of the multicast router. The range is 1 to 65535. The default value is 125 seconds.
`report-proxy <enable|disable>`	Enables or disables the IGMP report proxy feature. When enabled, reports are forwarded from hosts to the multicast router once per group per query interval. When disabled, all reports from different hosts are forwarded to multicast routers, which means that more than one group report may be forwarded for the same multicast group per query interval. The default is enabled.
`robust-value <integer>`	Robust value is used to determine group membership timeouts. It should be set to that of the multicast router in the network (range: 2 to 255). The default is 2.

config vlan <vid> igmp-snoop followed by:	
sender flush <*Group/IP Address*> [<*ports*>] [<*Host/IP Address*>]	Deletes IGMP senders for the specified groups. This action takes place immediately.
state <*enable*|*disable*>	Enables or disables the IGMP snooping feature. IGMP snooping will work only when a multicast router exists in the VLAN. If multicasting is enabled, but the VLAN does not hear a query from a multicast router, then the group reports from the hosts will not be processed.
static-members <*GroupAddress*> add <*ports*> <*static*|*blocked*>	Adds static member ports to the IGMP snooping group address and configures them as static (members) or blocked (not allowed to join).
static-members <*GroupAddress*> create <*ports*> <*static*|*blocked*>	Creates a static IGMP snooping group address with the specified ports as static (members) or blocked (not allowed to join). You can create a static entry without any ports so that if there is at least one multicast router in the VLAN, multicast data will be forwarded to that router. If there are no multicast routers in the VLAN and no port was entered in the static entry, the multicast data will be dropped. Subsequently, when a multicast router is learned or configured, the multicast data for this static entry will be forwarded to that router.
static-members <*GroupAddress*> delete	Deletes a static IGMP snooping group.
static-members <*GroupAddress*> info	Displays information about the static IGMP snooping group.
static-members <*GroupAddress*> remove <*ports*> <*static*|*blocked*>	Removes static member ports from the IGMP snooping group address and configures them as static (members) or blocked (not allowed to join).

Figure 86 config vlan igmp-snoop info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                    mrouter :
              query-interval : 125
                report-proxy : enable
                robust-value : 2
                       state : disable
```

show vlan igmp-snoop commands

The **show vlan igmp-snoop** commands display information about the IGMP snooping feature used to optimize data flow within all or a selected VLAN.

show vlan info snoop command

The **show vlan info snoop** command shows the IGMP snoop parameters configured for all or specified VLANs.

The command syntax is:

`show vlan info snoop [<vid>]`

Figure 87 shows output for the **show vlan info snoop** command.

Figure 87 show vlan info snoop command output

```
================================================================================
                                    Vlan Snoop
================================================================================
    IGMP  PROXY         QUERY  MROUTER ACT_RTR LAST            QUERIER   VLAN
VID SNOOP ENABLE ROBUST INTVAL PORTS   PORTS   QUERIER         PORT  EXP NAME
--------------------------------------------------------------------------------
1   false true   2      125                   0  .0  .0  .0         0   Default

2   false true   2      125                   0  .0  .0  .0         0   VLAN-2

45  false true   2      125                   0  .0  .0  .0         0   MM-16

75  false true   2      125                   0  .0  .0  .0         0   ubs

76  false true   2      125                   0  .0  .0  .0         0   vines

77  false true   2      125                   0  .0  .0  .0         0   ipx802d
ot2
78  false true   2      125                   0  .0  .0  .0         0   brouter
```

show vlan igmp-snoop access-list command

The **show vlan igmp-snoop access-list** command displays the access list for a specified VLAN ID.

The command syntax is:

`show vlan igmp-snoop access-list <vid> [<Group Address>]`

Figure 88 shows output for the **show vlan igmp-snoop access-list** command.

Figure 88 show vlan igmp-snoop access-list command output

```
================================================================================
                                  Vlan Igmp Snoop Access List
================================================================================
VLANID  GROUP           HOST ADDRESS    DENYACCESSMODE(s)
--------------------------------------------------------------------------------
```

show vlan igmp-snoop all-access-list command

The **show vlan igmp-snoop all-access-list** command has the same display as the **show vlan igmp-snoop access-list** command (Figure 88), except it displays all access lists, instead of only a specified VLAN ID.

show vlan igmp-snoop groups command

The **show vlan igmp-snoop groups** command displays information about the IGMP-snoop groups for all or specified VLANs.

The command syntax is:

```
show vlan igmp-snoop groups [<vid>]
```

Figure 89 shows output for the **show vlan igmp-snoop groups** command.

Figure 89 show vlan igmp-snoop groups command output

```
================================================================================
                                  Vlan Igmp Snoop Group
================================================================================
VLANID  GROUP           PORT  MEMBER           EXPIRE(s)  TYPE
--------------------------------------------------------------------------------
```

show vlan igmp-snoop senders info

The **show vlan igmp-snoop senders info** command displays information about the configured IGMP sender (source).

The command syntax is:

```
show vlan igmp-snoop senders info [<vid>]
```

Figure 90 shows output for the **show vlan igmp-snoop senders info** command.

Figure 90 show vlan igmp-snoop senders info command output

```
================================================================================
                                  Vlan Igmp Snoop Info Sender
================================================================================
VLANID  GROUP           PORT            HOST ADDRESS
--------------------------------------------------------------------------------
```

show vlan igmp-snoop static

The **`show vlan igmp-snoop static`** command uses the format `show vlan igmp-snoop static [<vid>]`. This command displays information about the static IGMP groups for all VLANs or for the specified VLAN (Figure 91).

Figure 91 show vlan igmp-snoop static command output

```
================================================================================
                                  Vlan Igmp Snoop Static
================================================================================
VLANID  GROUP           STATIC PORT(s)                  BLOCKED PORT(s)
--------------------------------------------------------------------------------
```

config vlan static-mcastmac

The **`config vlan static-mcastmac`** command is used to configure multicast MAC filtering.

`config vlan <vid> static-mcastmac` followed by:	
`add mac <value> [ports <value>] [mlt <value>]`	Adds VLSAN static multicast MAC entries, where: • mac <*value*> is the MAC address. • ports <*value*> are the ports to receive the multicast flooding. • mlt <value is the MID.
`add mlt <mid> mac <value>`	Adds MLT to VLAN static multicast MAC entries.
`add-ports <ports> mac <value>`	Adds ports to VLAN static multicast MAC entries.
`delete mac <value>`	Deletes VLAN static multicast MAC entries.
`delete-mlt <mid> mac <value>`	Deletes MLT-to-VLAN static multicast MAC entries.

config vlan <vid> static-mcastmac followed by:	
`delete-ports <ports> mac <value>`	Deletes ports from VLAN static multicast MAC entries.
`info`	Displays current settings.

Chapter 6
Configuring layer 3 protocol features

This chapter describes the CLI commands used to configure layer 3 (routing) functions in the Passport 1000 Series switch. This chapter includes sections about the following command groups used to configure routing characteristics:

- "IP routing commands," next
- "IP ARP commands" on page 188
- "DHCP relay commands" on page 196
- "UDP commands" on page 203
- "RIP commands" on page 208
- "OSPF commands" on page 218
- "VRRP commands" on page 240
- "IP multicast commands" on page 246
- "DVMRP commands" on page 249
- "Layer 3 IGMP commands" on page 257
- "IPX commands" on page 263

IP routing commands

The general **`IP routing`** commands allow you to enable and disable IP forwarding (routing) on the switch, ports, or VLAN.

config ip commands

The general **config ip** commands use the following options:

config ip followed by:	
info	Displays current default time-to-live characteristics (Figure 92).
default-ttl <*seconds*>	Sets the default time to live value for routing, the maximum number of seconds before a packet is discarded. The default value inserted in the ttl field whenever one is not supplied in the datagram header. Range is 1 to 255.
route delete <*ipaddr*|*mask*>	Deletes an IP route from a routing table.
forwarding disable	Disables IP forwarding (routing) on the entire switch. IP routing is disabled, allowing you to manage a Passport switch over a network without forcing the switch to also perform routing. Default is disable.
forwarding enable	Enables IP forwarding (routing) on the entire switch.
forwarding info	Displays IP forwarding status (Figure 93).
mroute interface <*ipaddr*> ttl <*ttl*>	Sets the default time-to-live for the multicast route interface.
route-discovery disable	Disables Internet Router Discovery Protocol (IRDP). This command will be fully implemented in a future release.
route-discovery enable	Enables IRDP. This command will be fully implemented in a future release.
route-discovery info	Displays route discovery status (Figure 94).
route info	Displays an IP routing table.
static-route create <*ipaddr/mask*> next-hop <*value*> [cost <*value*>]	Adds a static or default route to the switch: • ipaddr/mask is the IP address and mask for the route's destination. • next hop value is the IP address of the next hop router, the next router that packets must arrive at on this route. • cost is the metric of the route.
static-route delete <*ipaddr/mask*> <*value*>	Deletes a static route.
static-route disable <*ipaddr/mask*> <*value*>	Disables a static route.

config ip followed by:	
static-route enable <*ipaddr/mask*> <*value*>	Enables a static route.
static-route info	Displays characteristics of the created static route (Figure 95).

Figure 92 config ip info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

           icmp-net-unreach : disable
                default-ttl : 255
```

Figure 93 config ip forwarding info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                     enable : true
```

Figure 94 config ip route-discovery info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                      enable : false
```

Figure 95 config ip static-route info command output

```
create :
                    - 0.0.0.0/0.0.0.0
          next-hop - 10.10.40.1
              cost - 1
            status - ACTIVE
            enable - TRUE


disable : N/A

 delete : N/A

 enable : N/A
```

show ip commands

The **`show ip`** commands display the general IP characteristics of the switch.

show ip forwarding command

The **`show ip forwarding`** command displays the status of IP forwarding (routing) on the switch.

Figure 96 shows output for the **`show ip forwarding`** command.

Figure 96 show ip forwarding command output

```
IP Forwarding is enabled
IP Default TTL is 255 seconds
IP ARP life time is 360 minutes
```

show ip interface command

The **`show ip interface`** command displays the IP interfaces on the switch.

Figure 97 shows output for the **`show ip interface`** command.

Figure 97 show ip interface command output

```
================================================================================
                                    Ip Interface
================================================================================
INTERFACE IP              NET             BCASTADDR  REASM
          ADDRESS         MASK            FORMAT     MAXSIZE
--------------------------------------------------------------------------------
Port3/13  192.168.30.168  255.255.255.0   ones       1500
Port3/15  192.168.10.168  255.255.255.0   ones       1500
Vlan1     10.10.40.168    255.255.255.0   ones       1500
Vlan45    192.168.60.168  255.255.255.0   ones       1500
Vlan78    168.192.10.168  255.255.255.0   ones       1500
```

show ip route-discovery command

The **`show ip route-discovery`** command shows whether or not route discovery is enabled on the device.

Figure 98 shows output for the **`show ip route-discovery`** command.

Figure 98 show ip route-discovery command

```
Router Discovery Disabled
```

show ip route info command

The **`show ip route info`** command displays the existing IP route for the switch or for a specific net or subnet.

The command syntax is:

`show ip route info [<ip address>]{-s <value>]`

where:

`<ip address>` is the specific net (1.2. = 1.2.0.0) {a.b.c.d}.

`-s <value>` is the specific subnet {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.

Figure 99 shows output for the **show ip route info** command.

Figure 99 show ip route info command output

```
================================================================================
                                  Ip Route
================================================================================
            DST             MASK            NEXT COST VLAN   PORT  CACHE OWNER
--------------------------------------------------------------------------------
        0.0.0.0         0.0.0.0      10.10.40.1    1    1   3/1    TRUE STATIC
     10.10.40.0   255.255.255.0    10.10.40.168    1    1   -/-    TRUE  LOCAL
   192.168.30.0   255.255.255.0  192.168.30.168    1    -   3/13   TRUE  LOCAL
Total 3
```

config ip diffserv-rule commands

The general **config ip diffserve-rule** commands set Type of Service bits for Differentiated Services, providing an architecture for scalable service differentiation in the Internet. The Differentiated Services (DiffServ) specification defines a code point, which is a 6-bit value, known as the 8-bit Type of Service (TOS) field in an IP protocol header. In the DiffServ architecture, setting this code point provides a means of delivering a differentiated or better class of service for the IP packets.

To enable TOS-based high-priority mode using the CLI:

1. Enable the High Priority mode on the switch by entering:

   config sys set flags highpriomode true

2. Reboot the switch.
3. Enable TOS-based high-priority mode by entering:

   config ip diffserv tos-priority enable

   The default enabled threshold value is 3; so the threshold is set to 3.

4 To change the threshold value from 3 to a value between 0 (highest priority) and 7 (no priority), enter:

config ip diffserv tos-threshold *<integer>*

Note: The previous implementation of DiffServ (as explained in the *Reference for the Accelar 1000 Series Command Line Interface Software Release 2.0*) required the **config ip diffserv rule** command.

Passport release 2.1 software provides the capability of using an IP filter to set the decimal values that are used in an IP protocol filter to set the DiffServ bits on an IP frame. The DiffServ AND rule is first applied to the 8-bit field and acts as a mask. This value is used to protect or mask previously set bits. The DiffServ OR rules provide three values that can be used to set the DiffServ bits.

Note: Differentiated Services requires -B (ARU3) hardware.

The rule is selected using the command:

```
config ip traffic-filter filter <fid> modify diffserv-rule
<none|rule1|rule2|rule3>
```

For more information, refer to page 301.

The selected rule is logically ORed with the intermediate result after the original ANDing. The result is set as the new DiffServ code point in the IP header of the filtered frame. Table 11 shows how setting these values changes the TOS value.

Table 11 TOS values

Setting	Decimal	Binary
Original TOS value	37	00100101
AND rule	243	11110011
Intermediate result	33	00100001
OR rule	24	00011000
New TOS value	57	00111001

The **config ip diffserv** commands use the following options:

config ip diffserv followed by:	
and-mask <*integer*>	The AND rule mask value (0 to 255). The default is 0.
info	Displays diffserve settings.
or-rule1 <*integer*>	The first diffserv OR rule integer (0 to 255). The default is 0.
or-rule2 <*integer*>	The second diffserv OR rule integer (0 to 255). The default is 0.
or-rule3 <*integer*>	The third diffserv OR rule integer (0 to 255). The default is 0.
tos-priority enable	Enables TOS-based high priority mode.
tos-threshold <*integer*>	Changes the threshold value from 3 to a value between 0 (highest priority) and 7 (no priority).

show ip diffserv command

The **show ip diffserv** command displays the settings for the Passport switch release 2.0 **diffserv** commands and the Passport switch release 2.1 TOS-based high-priority forwarding.

Figure 100 shows output for the **show ip diffserv** command.

Figure 100 show ip diffserv command output

```
================================================================================
                                    Ip Tos Rule
================================================================================
and-mask              : 0
or-rule1              : 0
or-rule2              : 0
or-rule3              : 0
tos-priority          : disable
tos-threshold         : 0
```

ethernet ports ip commands

The **ethernet ports ip** commands are generic port-related IP routing commands. Other port commands are included in the section dealing with the protocol or feature, for example, DHCP.

config ethernet ports ip command

In order for the **config ethernet ports ip** commands to take effect, IP forwarding must be enabled on the switch using the command:

config ip forwarding enable

The port commands require the parameter <*ports*> as the port or list of ports on which you are running the command {slot/port[-slot/port][, ...]}.

The **config ethernet ports ip** commands use the following options:

config ethernet <ports> ip followed by:	
directed-broadcast enable	Enables directed broadcasts on an isolated routing port.
directed-broadcast disable	Disables directed broadcasts on an isolated routing port.
directed-broadcast info	Displays directed broadcast settings on an isolated routing port.
info	Displays configured IP characteristics on the port (Figure 101).
create-brouter <*ipaddr/mask*> <*tag-id*>	Creates a brouter port (single-port VLAN) at the specified IP address and subnet mask, with the specified tag ID.
create <*ipaddr/mask*>	Assigns an IP address to a port. Assigning an IP address to a port creates an isolated routing port, removing it from any existing VLAN.
delete <*ipaddr*>	Deletes an IP address from an isolated routing port.

Figure 101 config ethernet ip info command output

```
Sub-Context: clear config monitor show test trace
Current Context:
```

show ports info ip

The **`show ports info ip`** command displays routing (IP) information for all or specified ports.

The command syntax is:

`show ports info ip [<ports>]`

Figure 102 shows output for the **`show ports info ip`** command.

Figure 102 show ports info ip command output

```
================================================================================
                                    Port Ip
================================================================================
PORT     IP_ADDRESS       NET_MASK         BROADCAST  REASM   ADVERTISE  DIRECT
NUM                                                   MAXSIZE WHEN_DOWN  BCAST
--------------------------------------------------------------------------------
3/2      168.192.10.168   255.255.255.0    ones       1500    disable    enable

3/13     192.168.30.168   255.255.255.0    ones       1500    disable    enable

3/15     192.168.10.168   255.255.255.0    ones       1500    disable    enable
```

vlan ip commands

The **`vlan ip`** commands are general routing commands on the VLAN. Other VLAN commands are included in the sections dealing with protocols or features, for example, DHCP.

config vlan ip command

The general **`config vlan ip`** commands require a VLAN ID <*vid*> from 1 to 4095.

The **config vlan ip** command uses the following options:

config vlan <vid> ip followed by:	
directed-broadcast enable	Enables directed broadcasts on a VLAN.
directed-broadcast disable	Disables directed broadcasts on a VLAN.
directed-broadcast info	Displays directed broadcast settings on a VLAN.
info	Displays VLAN routing characteristics (Figure 103).
advertise-when-down <*enable*|*disable*>	Sets whether to advertise the network on this VLAN, even if the VLAN is down (no active ports). The default is disabled. **Note**: When you create a new VLAN without any link and enable advertise-when-down, it will not advertise your route until a port is active in the VLAN. Then the route will be advertised even when the link is down. To disable advertising based on link status, this parameter should be disabled.
create <*ipaddr/mask*>	Assigns an IP address and subnet mask to the VLAN.
delete <*ipaddr*>	Deletes the specified VLAN address.

Figure 103 config vlan ip info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                    create : 10.10.40.168/255.255.255.0
                    delete : N/A
```

show vlan info ip command

The **show vlan info ip** command displays the routing (IP) configuration for all or specified VLANs.

The command syntax is:

```
show vlan info igmp [<vid>]
```

Figure 104 shows output for the **show vlan info ip** command.

Figure 104 show vlan info ip command output

```
================================================================================
                                    Vlan Ip
================================================================================
VLAN            IP              NET             BCASTADDR REASM    ADVERTISE
ID   NAME       ADDRESS         MASK            FORMAT    MAXSIZE  WHEN_DOWN
--------------------------------------------------------------------------------
1    Default    10.10.40.168    255.255.255.0   ones      1500     disable
45   MM-16      192.168.60.168  255.255.255.0   ones      1500     disable
78   brouter    168.192.10.168  255.255.255.0   ones      1500     disable


================================================================================
                                Vlan Ip Continued
================================================================================
DIRECTED
BROADCAST
--------------------------------------------------------------------------------
enable
enable
enable
```

IP ARP commands

The Address Resolution Protocol (ARP) commands enable you to add and delete static entries in the ARP table and to display the ARP table. The ARP table maps MAC addresses to IP addresses. If you add an ARP entry for a VLAN, the VLAN is associated with the MAC address you specify. When you display the ARP table, all entries (static and dynamic) are displayed. Before you can add an ARP entry to a port or port-based VLAN, an IP address must already be assigned to the port or VLAN and routing must be enabled.

config ip arp commands

The **config ip arp** commands configure ARP on the switch and use the following options:

config ip arp followed by:	
info	Displays ARP characteristics (Figure 105).
add ports <*value*> ip <*value*> mac <*value*> [vlan<*value*>]	Adds a static entry to the ARP table. • ports <value> are the port numbers, shown as slot/port. • ip <value> is the IP address (a.b.c.d.). • mac <value> is the 48-bit hardware MAC address in the format 0x00:0x00:0x00:0x00:0x00:0x00. • vlan <value> is the name or number of a VLAN.
aging <*seconds*>	Sets the length of time in seconds an entry will remain in the ARP table before timeout. Range is 1 to 32767.
delete <*ipaddr*>	Removes an entry from the ARP table.

Figure 105 config ip arp info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                        aging : 360
                       delete : N/A
                          add :
                                  ports - 3/1
                                     ip - 10.10.40.120
                                    mac - 08:00:20:8f:69:b7
                                   vlan - 1

                                  ports - 3/1
                                     ip - 10.10.40.209
                                    mac - 00:80:2d:22:0e:00
                                   vlan - 1

                                  ports - 3/1
                                     ip - 10.10.40.136
                                    mac - 00:e0:16:a2:c2:00
                                   vlan - 1

                                  ports - 3/1
                                     ip - 10.10.40.126
                                    mac - 08:00:20:87:60:8b
                                   vlan - 1
```

config ip arp static-mcastmac

Use the **config ip arp static-mcastmac** command to add, delete, and display multicast MAC entries.

config ip arp static-mcastmac followed by	
ad mac <*value*> ip <*value*> vlan <*value*> [ports <*value*>] [mlt <*value*>]	Adds static multicast MAC entries, where: • mac <*value*> is the MAC address. • ip <*value*> is the IP address. • vlan <*value*> is the VLAN ID number. • ports <*value*> are the ports to receive the multicast flooding. • mlt <*value*> is the MID.
delete <*ipaddr*>	Deletes static multicast MAC entries.
info	Displays current settings.

Note: If the user creates an ARP entry for which there is not an existing multicast MAC address on the VLAN > Snoop > Multicast tab, the software creates an L2 multicast MAC address entry.

show ip arp commands

The show ip arp commands display ARP configuration on the switch.

show ip arp info command

The **`show ip arp info`** command displays the ARP table.

The command syntax is:

`show ip arp info [<ip address>] [-s <value>]`

where:

`<ip address>` is the specific net IP address for the table .

`[-s <value>]` is the specific subnet in the format `(a.b.c.d/x|a.b.c.d/x.x.x.x|default)`.

Figure 106 shows output for the **`show ip arp info`** command.

Figure 106 show ip arp info command output

```
================================================================================
                                    Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE     TTL
--------------------------------------------------------------------------------
10.10.40.91     00:80:5f:e7:e4:39  1       3/1   DYNAMIC 2153
10.10.40.161    08:00:20:79:0a:f3  1       3/1   DYNAMIC 2130
10.10.40.84     08:00:20:8d:7c:d6  1       3/1   DYNAMIC 2113
10.10.40.120    08:00:20:8f:69:b7  1       3/1   DYNAMIC 2102
10.10.40.209    00:80:2d:22:0e:00  1       3/1   DYNAMIC 2093
10.10.40.136    00:e0:16:a2:c2:00  1       3/1   DYNAMIC 2093
10.10.40.126    08:00:20:87:60:8b  1       3/1   DYNAMIC 2082
10.10.40.67     00:e0:16:00:00:00  1       3/1   DYNAMIC 2063
10.10.40.95     00:80:2d:af:8b:f4  1       3/1   DYNAMIC 2063
10.10.40.94     00:80:2d:35:df:f4  1       3/1   DYNAMIC 2063
10.10.40.151    00:00:81:c1:f6:81  1       3/1   DYNAMIC 2050
10.10.40.219    00:80:2d:06:e5:92  1       3/1   DYNAMIC 2031
10.10.40.86     00:80:5f:3f:e4:f0  1       3/1   DYNAMIC 2023
10.10.40.152    00:00:81:c1:9b:81  1       3/1   DYNAMIC 2020
10.10.40.23     00:e0:16:53:bc:00  1       3/1   DYNAMIC 1996
10.10.40.51     00:80:2d:22:87:f4  1       3/1   DYNAMIC 1993
10.10.40.102    08:00:20:74:a0:ab  1       3/1   DYNAMIC 1982
10.10.40.101    08:00:20:8e:1a:ef  1       3/1   DYNAMIC 1963
10.10.40.235    00:60:fd:9e:2b:6b  1       3/1   DYNAMIC 1938
```

ethernet ip arp commands

The **`ethernet ip arp`** commands are the port IP ARP commands. These commands require the parameter `<ports>` as the port or list of ports on which the command is running.

The command syntax is:

`{slot/port[-slot/port][, ...]}`

config ethernet ip arp command

The **config ethernet ip arp** command uses the following options:

config ethernet <ports> ip followed by:	
arp-response disable	Disables ARP responses on the port.
arp-response enable	Enables ARP responses on the port.
arp-response info	Displays ARP response status on the port (Figure 107).
proxy disable	Disables proxy ARP on the port.
proxy enable	Enables proxy ARP on the port, allowing a router to answer a local ARP request for a remote destination.
proxy info	Displays ARP proxy status on the port (Figure 108).

Figure 107 config ethernet ip arp-response info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

Port 3/1 :
                arp-response : enable
```

Figure 108 config ethernet ip proxy info command

```
Sub-Context: clear config monitor show test trace
Current Context:

Port 3/1 :
                      proxy : disable
```

show ports info arp command

The **show ports info arp** command displays ARP information for a specified port or all ports.

The command syntax: is:

```
show ports info arp [<ports>]
```

Figure 109 shows output for the **show ports info arp** command.

Figure 109 show ports info arp command output

```
================================================================================
                                    Port Arp
================================================================================
PORT_NUM DOPROXY    DORESP
--------------------------------------------------------------------------------
3/1      false      true
3/2      false      true
3/3      false      true
3/4      false      true
3/5      false      true
3/6      false      true
3/7      false      true
3/8      false      true
3/9      false      true
3/10     false      true
3/11     false      true
3/12     false      true
3/14     false      true
3/16     false      true
```

vlan ip arp general commands

The **vlan ip arp general** commands for VLAN ARP require a VLAN ID <*vid*> from 1 to 4095.

config vlan ip arp command

The general configuration commands for VLAN ARP use the following options:

config vlan <vid> ip followed by:	
`proxy disable`	Disables proxy ARP on the VLAN. This is the default state.
`proxy enable`	Enables proxy ARP on the VLAN.
`proxy info`	Displays VLAN proxy ARP status (Figure 110).

config vlan <vid> ip followed by:	
`resp disable`	Disables ARP response on the VLAN.
`resp enable`	Enables ARP response on the VLAN. This state is the default state.
`resp info`	Displays VLAN ARP response status (Figure 111).

Figure 110 config vlan ip proxy info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                        proxy : disable
```

Figure 111 config vlan ip resp info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                        resp : enable
```

show vlan info arp command

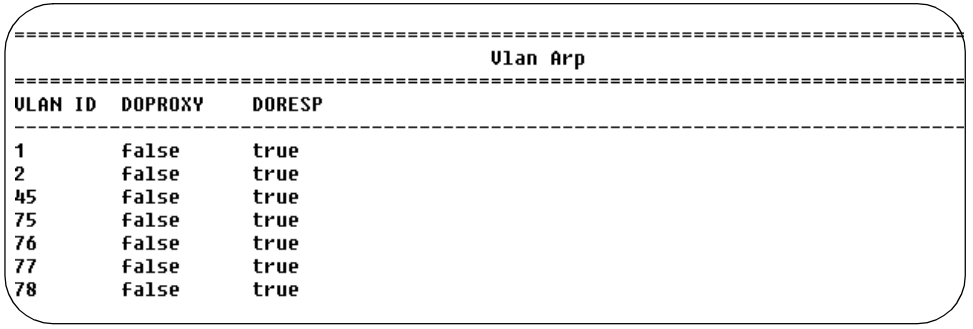
The **`show vlan info arp`** command displays the ARP configuration for all VLANs or specified VLANs.

The command syntax is:

`show vlan info arp [<vid>]`

Figure 112 shows output for the **`show vlan info arp`** command.

Figure 112 show vlan info arp command output



```
================================================================================
                                    Vlan Arp
================================================================================
VLAN ID  DOPROXY    DORESP
--------------------------------------------------------------------------------
1        false      true
2        false      true
45       false      true
75       false      true
76       false      true
77       false      true
78       false      true
```

DHCP relay commands

The Dynamic Host Configuration Protocol (DHCP), an extension of the Bootstrap Protocol (BootP), is used to dynamically provide host configuration information to workstations. Use the port DHCP relay commands to set DHCP relay behavior on an isolated routing port. Use the VLAN DHCP commands to set DHCP relay behavior on a VLAN.

You must enable DHCP relay on the path for port or VLAN configuration to take effect.

config ip dhcp-relay commands

The **config ip dhcp-relay** commands allow you to view and configure DHCP parameters globally and uses the following options:

config ip dhcp-relay followed by:	
info	Displays current DHCP global configuration on the switch.
create-fwd-path agent <*value*> server <*value*> [mode <*value*>] [state <*value*>]	Configures the forwarding path from the client to the server. • The agent is the IP address configured on an interface (a locally configured IP address). • The server is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out the interface. • Mode is to forward BootP messages only, DHCP messages only, or both. • State is enable, disable, or delete the forwarding path.
enable-fwd-path agent <*value*> server <*value*>	Enables DHCP relaying on the path from the IP address to the server.
delete-fwd-path agent <*value*> server <*value*>	Deletes the forwarding path from the client to the server.
disable-fwd-path agent <*value*> server <*value*>	Disables DHCP relaying on the path from the IP address to the server. This is the default.
mode <*mode*> agent <*value*> server <*value*>	Modifies DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

show ip dhcp commands

The **show ip dhcp** commands display DHCP routing information.

show ip dhcp fwd-path command

The **show ip dhcp fwd-path** command displays DHCP routing information, including interface, server, enabled, disabled, and mode (forward BootP messages only, DHCP messages only, or both).

show ip dhcp counters command

The **show ip dhcp counters** command displays DHCP counter information, including the number of requests and replies for each interface.

config ethernet ip dhcp-relay commands

The **config ethernet ip dhcp-relay** commands allow you to view and configure DHCP parameters on specified isolated routing ports.The port commands require the parameter <ports> as the port or list of ports on which you are running the command.

The command syntax is:

```
{slot/port[-slot/port][, ...]}
```

The **config ethernet ip dhcp-relay** commands use the following options:

config ethernet <ports> ip dhcp-relay followed by:	
info	Displays the current port DHCP configuration (Figure 113).
broadcast <*enable*|*disable*>	Sets whether the server reply is sent as a broadcast or unicast back to the end station.
disable	Disables DHCP relaying on the port.This is the default state.
enable	Enables DHCP relaying on the port.
max-hop <*max-hop*>	Sets the maximum number of hops before a BootP/DHCP packet is discarded (1 to 16). The default is 4.

config ethernet <ports> ip dhcp-relay followed by:	
min-sec <*min-sec*>	Sets the minimum seconds count set for DHCP. If the “secs” field in the BootP/DHCP packet header is greater than this value, the switch relays or forwards the packet; otherwise, the packet is dropped (0 to 65535). The default is 0 seconds.
mode <*mode*>	Sets DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

Figure 113 config ethernet ip dhcp-relay info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

Port 3/1 :
                  dhcp-relay : disable
                   broadcast : disable
                    learnarp : disable
                      max-hop : 4
                      min-sec : 0
                         mode : both
```

show port dhcp commands

The **show port dhcp** commands display information about DHCP on the port.

show ports info dhcp command

The **show ports info dhcp** command displays the DHCP parameters for all ports or a specified port.

The command syntax is:

```
show ports info dhcp [<ports>]
```

Figure 114 shows output for the **show ports info dhcp** command.

Figure 114 show ports info dhcp command output

```
================================================================================
                                    Port Dhcp
================================================================================
PORT_NUM ENABLE   MAX_HOP  MIN_SEC  MODE  ALWAYS_BROADCAST     LEARN_ARP

--------------------------------------------------------------------------------
3/1      false    4        0        both  false               false

3/2      false    4        0        both  false               false

3/3      false    4        0        both  false               false

3/4      false    4        0        both  false               false

3/5      false    4        0        both  false               false

3/6      false    4        0        both  false               false

3/7      false    4        0        both  false               false

3/8      false    4        0        both  false               false

3/9      false    4        0        both  false               false

3/10     false    4        0        both  false               false

3/11     false    4        0        both  false               false

3/12     false    4        0        both  false               false

3/13     false    4        0        both  false               false

3/14     false    4        0        both  false               false

3/15     false    4        0        both  false               false

3/16     false    4        0        both  false               false
```

show ports stats dhcp

The **show ports stats dhcp** command displays DHCP statistics for all ports or a specified port.

The command syntax is:

```
show ports stats dhcp [<ports>]
```

Figure 115 shows output for the **show ports stats dhcp** command.

Figure 115 show ports stats dhcp command output

```
================================================================================
                                    Port Stats Dhcp
================================================================================
PORT_NUM NUMREQUEST NUMREPLY
--------------------------------------------------------------------------------
3/1      0          0
3/2      0          0
3/3      0          0
3/4      0          0
3/5      0          0
3/6      0          0
3/7      0          0
3/8      0          0
3/9      0          0
3/10     0          0
3/11     0          0
3/12     0          0
3/13     0          0
3/14     0          0
3/15     0          0
3/16     0          0
```

config vlan ip dhcp-relay commands

The **`config vlan ip dhcp-relay`** commands configure DHCP routing on the VLAN. These commands require a VLAN ID `<vid>` from 1 to 4095 and use the following options:

`config vlan <vid> ip dhcp-relay` followed by:	
`info`	Displays DHCP characteristics on the VLAN (Figure 116).
`broadcast <enable|disable>`	Sets whether the server reply is sent as a broadcast back to the end station.
`disable`	Disables DHCP relaying on the VLAN. This is the default state.
`enable`	Enables DHCP relaying on the VLAN.
`max-hop <max-hop>`	Sets the maximum number of hops before the BootP/DHCP packet is dropped (1 to 16).

config vlan <vid> ip dhcp-relay followed by:	
min-sec <*min-sec*>	Sets the minimum seconds count for DHCP. If the secs field in the packet header is greater than this value, the switch forwards the packet.; otherwise, it is dropped (0 to 65535).
mode <*mode*>	Sets DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

Figure 116 config vlan ip dhcp-relay info command output

```
Sub-Context: clear config monitor show test trace
Current Context:

                  dhcp-relay : disable
                   broadcast : disable
                     learnarp : disable
                      max-hop : 4
                      min-sec : 0
                         mode : both
```

show vlan info dhcp command

The **show vlan info dhcp** command displays DHCP parameters for all or specified VLANs. The interface index (IF Index) is assigned as the VLAN is created. Numbers 1 to 256 are ports; numbers above 257 are VLANs.

The command syntax is:

```
show vlan info dhcp [<vid>]
```

Figure 117 shows output for the **show vlan info dhcp** command.

Figure 117 show vlan info dhcp command output

```
================================================================================
                                    Vlan Dhcp
================================================================================
VLAN IF            MAX    MIN           ALWAYS
ID   INDEX  ENABLE HOP    SEC    MODE    BCAST  LRNARP
--------------------------------------------------------------------------------
1    257    false  4      0      both    false  false
2    265    false  4      0      both    false  false
45   259    false  4      0      both    false  false
75   258    false  4      0      both    false  false
76   263    false  4      0      both    false  false
77   264    false  4      0      both    false  false
78   260    false  4      0      both    false  false
```

UDP commands

Some network applications, such as the NetBIOS name service, rely on a User Data Protocol (UDP) broadcast to request or locate a service. By default, broadcasts are not forwarded by a router. UDP broadcast forwarding is a generalized mechanism for the router to selectively forward UDP broadcasts.

The basic procedure for setting up UDP broadcast forwarding is:

- Use the **`config ip udpfwd protocol`** commands to enter protocols in a protocol table.
- Use the **`config ip udpfwd portfwdlist`** commands to create and name the port forward list and assign protocols and servers to the port forward list.
- Use the **`config ip interface`** commands to apply the port forward list to the appropriate interfaces.

The **`config ip udpfwd info`** command displays the current UDP forwarding configuration.

config ip udpfwd protocol command

Use the **`config ip udpfwd protocol`** command to enter protocols in a protocol table.

The UDP forwarding protocol command requires the `<udpport>` parameter as the UDP protocol port number (1 to 255).

The **`config ip udpfwd protocol`** command uses the following options:

`config ip udpfwd protocol <udpport>` followed by:	
`create <protoname>`	Creates a new UDP protocol where <protoname> is the UDP protocol name {string} .
`delete`	Deletes a UDP port protocol.
`info`	Displays created and/or deleted UDP protocols.

config ip udpfwd portfwdlist commands

The UDP forwarding port forward list commands require the `<fwdlist>` parameter as the port forwarding list number (1 to 1000).The commands use the following options:

`config ip udpfwd portfwdlist <fwdlist>` followed by:	
`add-portfwd <udpport> <ipaddr>`	Adds a UDP protocol port (1 to 255) to the specified port forwarding list.
`create`	Creates a UDP port forwarding list (1 to 1000).
`delete`	Deletes a port forward list ID.
`info`	Displays the current configuration for the port forward list ID.
`name <name>`	Assigns a name to the UDP port forwarding list.
`remove-portfwd <udpport> <ipaddr>`	Removes a protocol port forwarding entry and IP address from the list.

config ip udpfwd interface commands

The UDP forwarding interface commands require an IP address and use the following options:

config ip udpfwd interface <ipaddr> followed by:	
`info`	Displays the current UDP interface configuration.
`create <fwdlistid>`	Assigns a forwarding list ID to an interface IP address.
`delete`	Removes the forwarding list from the IP address.
`maxttl <maxttl>`	Sets maximum time-to-live for the UDP broadcast forwarded by the interface.
`udpportfwdlist <fwdlistid>`	Changes the port forwarding list.

show ip udpfwd commands

The **`show ip udpfwd`** commands display information about the UDP forwarding characteristics of the switch.

show ip udpfwd interface info command

The **`show ip udpfwd interface info`** command displays information about the UDP interface for the switch or a specified IP address.

The command syntax is:

```
show ip udpfwd interface info [<ipaddr>]
```

Figure 118 shows output for the **`show ip udpfwd interface info`** command.

Figure 118 show ip udpfwd interface info command output

```
================================================================================
                                  Udp Broadcast Interface Forwarding Tbl
================================================================================
INTF_ADDR       FWD    MAXTTL RXPKTS  FWDPKTS DRPTTLEX DRPDEST  DRP_UNKNOWN
                LISTID                                UNREACH  PROTOCOL
--------------------------------------------------------------------------------
```

show ip udpfwd portfwd info command

The **show ip udpfwd portfwd info** command displays the UDP port forwarding table.

Figure 119 shows output for the **show ip udpfwd portfwd info** command.

Figure 119 show ip udpfwd portfwd info command output

```
================================================================================
                                  Udp Port Fwd Tbl
================================================================================
UDP_PORT FORWARDING_ADDR FWDPKTS  DRPTTLEX DRPDEST_UNKNOWN
--------------------------------------------------------------------------------
```

show ip udpfwd portfwdlist info command

The **show ip udpfwd portfwdlist info** command displays the UDP Port Forwarding List Table for all or a specified list.

The command syntax is:

`show ip udpfwd portfwdlist info [<`*fwdlistid*`>]`

show ip udpfwd protocol info command

This **show ip udpfwd protocol info** command displays the UDP protocol table with the UDP port numbers for each supported or designated protocol.

Figure 120 shows output for the **show ip udpfwd protocol info** command.

Figure 120 show ip udpfwd protocol info command output

```
Passport 1100# show ip udpfwd protocol info

================================================================================
                                    Udp Protocol Tbl
================================================================================
UDP_PORT PROTOCOL_NAME
--------------------------------------------------------------------------------
37       Time Service
49       TACACS Service
53       DNS
69       TFTP
137      NetBIOS NameSrv
138      NetBIOS DataSrv
```

IP Static Routing Table Manager

In the CLI, the **`config ip static-route`** commands use the following options:

`config ip static-route` followed by:	
`create <ipaddr/mask> next-hop <value> cost <value>`	Adds new static routes, where: • *`ipaddr/mask`* is the IP address and mask of the route. • `next-hop` is the next hop IP address. • `cost` is the metric associated with the route.
`delete <ipaddr/mask> next-hop <value>`	Deletes a static route.
`disable <ipaddr/mask> next-hop <value>`	Disables a static route, but does not delete it from the table.
`enable <ipaddr/mask> next-hop <value>`	Enables a disabled static route.
`info`	Shows the current settings.

In the OWNER column of the IP Routing table (shown in Figure 121), an entry of “Static” indicates that it is a static route and, because it is found in the System Routing Table, the next-hop address of the static route is reachable.

Figure 121 show ip route info command output

```
Passport 1100# show ip route info

================================================================================
                                    Ip Route
================================================================================
          DST             MASK            NEXT COST VLAN   PORT  CACHE OWNER
--------------------------------------------------------------------------------

Total 5 routes
        0.0.0.0         0.0.0.0      10.10.40.1    1    1   3/1    TRUE STATIC
     10.10.40.0   255.255.255.0    10.10.40.168    1    1   -/-    TRUE  LOCAL
    10.168.40.0   255.255.255.0   10.168.40.168    1   75   -/-    TRUE  LOCAL
   10.168.168.0   255.255.255.0  10.168.168.168    1    3   -/-    TRUE  LOCAL
   192.168.30.0   255.255.255.0  192.168.30.168    1    -   3/13   TRUE  LOCAL

Total 5 printed_out of 5
```

RIP commands

This section describes the commands used to configure the Routing Information Protocol (RIP) on the Passport 1000 Series switch. RIP is configured on an isolated routing port or on a VLAN, but it must also be enabled globally.

config ip rip commands

The **`config ip rip`** commands allow you to globally enable or disable RIP on the switch and use the following options:

`config ip rip` followed by:	
`info`	Displays current RIP configuration settings (Figure 122).
`disable`	Globally disables RIP on the switch.
`domain <ipaddr> <value>`	Changes the RIP interface configuration domain, the value inserted into the routing domain field of all RIP packets sent on this interface. • *`ipaddr`* is the interface IP address {a.b.c.d}. • *`value`* is the domain value {0 to 39321}.
`enable`	Globally enables RIP on the switch.

config ip rip followed by:	
holddown <*seconds*>	Sets the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The range is 0 to 360, with a default of 120.
updatetime <*seconds*>	Sets RIP update timer, the time interval between RIP updates. The range is 0 to 360, with a default of 30 seconds.
receive <*ipaddr*> mode <*value*>	Changes the RIP interface receive configuration. IP address is the address of the interface, and mode indicates the RIP versions to accept: • rip1 = RIP version 1 • rip2 = RIP version 2 • rip1-or-rip2= receive in either RIP 1 or 2
send <*ipaddr*> mode <*value*>	Changes the RIP interface send configuration. IP address is the address of the interface, and mode indicates the RIP versions to send: • notsend = no RIP updates are sent • rip1 = RIP version 1 • rip1comp = broadcast RIP 2 updates • rip2 = multicast RIP 2 updates

Figure 122 config ip rip info command output

```
                enable : false
              holddown : 120
            updatetime : 30
                domain :
                                - 192.168.30.168
                                - 0
               receive :
                                - 192.168.30.168
                             mode - rip1OrRip2
                  send :
                                - 192.168.30.168
                             mode - rip1Compatible
                domain :
                                - 192.168.10.168
                                - 0
               receive :
                                - 192.168.10.168
                             mode - rip1OrRip2
                  send :
                                - 192.168.10.168
                             mode - rip1Compatible
                domain :
                                - 10.10.40.168
```

show ip rip commands

The **show ip rip** commands display information about the RIP configuration on the switch.

show ip rip info

The **show ip rip info** command displays the RIP global status on the switch.

Figure 123 shows output for the **show ip rip info** command.

Figure 123 show ip rip info command output

```
                Rip : Disabled
        Update Time : 30
      HoldDown Time : 120
      Route Changes : 0
            Queries : 0
             Domain : 0
                    _
```

show ip rip interface

The **show ip rip interface** command displays information about all RIP interfaces or a specified RIP interface.

The command syntax is:

`show ip rip interface [<ipaddr>]`

Figure 124 shows output for the **show ip rip interface** command.

Figure 124 show ip rip interface command output

```
Passport 1100# show ip rip interface

================================================================================
                                    Rip Interface
================================================================================
IP_ADDR         RIP_ENABLE      SEND                RECEIVE
--------------------------------------------------------------------------------
192.168.30.168  false           rip1Compatible      rip1OrRip2
192.168.10.168  false           rip1Compatible      rip1OrRip2
10.10.40.168    false           rip1Compatible      rip1OrRip2
192.168.60.168  false           rip1Compatible      rip1OrRip2
168.192.10.168  false           rip1Compatible      rip1OrRip2
```

config ethernet port ip rip commands

The **config ethernet port ip rip** commands configure RIP on specified isolated-routing ports. RIP must also be enabled globally for the commands to take effect. These commands use the <ports>parameter to specify the ports for which you are entering the command.

The command syntax is:

```
portlist {slot/port[-slot/port][, ...]}
```

The port-based RIP commands use the following options:

config ethernet <ports> ip rip followed by:	
info	Displays RIP characteristics on the port (Figure 125).
advertise-when-down <*enable*|*disable*>	If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. **Note**: When you configure a port without any link and enable advertise-when-down, it will not advertise your route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter should be disabled.

config ethernet <ports> ip rip followed by:	
auto-aggr <*enable*|*disable*>	Enables or disables automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disable.
default-listen <*enable*|*disable*>	Allows the user to enable or disable setting RIP listen to accept the default route via RIP.
disable	Disables RIP on the port. This setting is the default.
enable	Enables RIP on the port.
default-supply <*enable*|*disable*>	Allows the user to send a default route only if one exists in the routing table.
listen <*enable*|*disable*>	Configures whether the switch listens for a default route without listening for any other routes.
manualtrigger	Allows you to manually issue a RIP update.
poison <*enable*|*disable*>	Sets whether RIP routes on the port learned from a neighbor are advertised back to the neighbor. If disabled, split horizon is invoked and IP routes learned from an immediate neighbor are not advertised back to the neighbor. If enabled, the RIP updates sent to a neighbor from which a route is learned are “poisoned” with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network.
supply <*enable*|*disable*>	Configures whether the switch supplies (talk to) the default route without advertising any other routes.
trigger <*enable*|*disable*>	Enables or disables automatic triggered updates for RIP.

Figure 125 config ethernet ip rip info command output

```
Passport 1100# show ip rip interface

================================================================================
                                    Rip Interface
================================================================================
IP_ADDR         RIP_ENABLE      SEND                RECEIVE
--------------------------------------------------------------------------------
192.168.30.168  false           rip1Compatible      rip1OrRip2
192.168.10.168  false           rip1Compatible      rip1OrRip2
10.10.40.168    false           rip1Compatible      rip1OrRip2
192.168.60.168  false           rip1Compatible      rip1OrRip2
168.192.10.168  false           rip1Compatible      rip1OrRip2

Passport 1100# config ethernet ip rip info
object <ports> = ip is out of range
object <ports> required
<ports>          = portlist {slot/port[-slot/port][,...]}

port commands
auto-negotiate  set auto-negotiate
default-vlan-id set default vlan id
duplex          set duplex
high-priority   set high priority for a port
info            show current level parameter settings and next level directories
ip              port ip commands
linktrap        set link up/down trap
lock            set lock
oversize-frame  set oversized frame
perform-tagging set perform tagging option
preferred-phy   set preferred connector to a port
speed           set speed
state           set port state up/down/test
stg             set port stg commands
tagged-frames-discardset discard tagged frames
unknown-mac-discarddiscard unknown source mac frames commands
untagged-frames-discardset discard untagged frames
```

Table 12 indicates the relationship between switch action and the RIP supply and listen settings.

Table 12 RIP supply and listen settings and switch action

RIP Supply settings		RIP Listen settings		
Supply	**Default supply**	**Listen**	**Default listen**	**Switch action**
Disabled	Disabled			Sends no RIP updates.
Enabled	Disabled			Sends RIP updates except the default.
Disabled	Enabled			Sends only the default (default route must exist in routing table).
Enabled	Enabled			Sends RIP updates including the default route (if it exists).
		Disabled	Disabled	Does not listen for RIP updates.
		Enabled	Disabled	Listens for all RIP updates except the default.
		Disabled	Enabled	Listens only for the default.
		Enabled	Enabled	Listens for RIP updates including the default route (if it exists).

show ports info rip command

The **`show ports info rip`** command displays information about the RIP parameters for all ports or a specified port.

The command syntax is:

```
show ports info rip [<ports>]
```

Figure 126 shows output for the **`show ports info rip`** command.

Figure 126 show ports info rip command output

```
Passport 1100# show ports info rip

================================================================================
                                    Port Rip
================================================================================
PORT         ADVERTISE ACCEPT  TRIGGERED AUTOAGG
NUM   ENABLE DEFAULT   DEFAULT UPDATE    ENABLE  SUPPLY LISTEN POISON
--------------------------------------------------------------------------------
3/1   false  false     false   false     false   true   true   false
3/2   false  false     false   false     false   true   true   false
3/3   false  false     false   false     false   true   true   false
3/4   false  false     false   false     false   true   true   false
3/5   false  false     false   false     false   true   true   false
3/6   false  false     false   false     false   true   true   false
3/7   false  false     false   false     false   true   true   false
3/8   false  false     false   false     false   true   true   false
3/9   false  false     false   false     false   true   true   false
3/10  false  false     false   false     false   true   true   false
3/11  false  false     false   false     false   true   true   false
3/12  false  false     false   false     false   true   true   false
3/13  false  false     false   false     false   true   true   false
3/14  false  false     false   false     false   true   true   false
3/15  false  false     false   false     false   true   true   false
3/16  false  false     false   false     false   true   true   false
```

config vlan ip rip commands

The **`config vlan ip`** commands set RIP parameters for a VLAN, where `<vid>` is the VLAN ID (1 to 4095).

The **`config vlan ip`** commands use the following options:

`config vlan <vid> ip rip` followed by:	
`info`	Displays RIP characteristics on the VLAN (Figure 127).
`advertise-when-down <enable|disable>`	If enabled, the network on this interface is advertised as up, even if no ports in the VLAN are active. The default is disabled. **Note**: When you create a VLAN with no active ports and enable advertise-when- down, it will not advertise your route until a port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter should be disabled.

config vlan <vid> ip rip followed by:	
auto-aggr <*enable*|*disable*>	Enables or disables automatic route aggregation on the VLAN. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disable.
default-listen <*enable*|*disable*>	Allows the user to enable or disable setting RIP listen to accept the default route via RIP.
default-supply <*enable*|*disable*>	Disables RIP on the VLAN. This is the default setting.
disable	Enables RIP on the VLAN.
enable	Allows the user to send a default route only if one exists in the routing table.
listen <*enable*|*disable*>	Configures whether the switch listens for a default route without listening for any other routes.
manualtrigger	Allows you to manually issue a RIP update.
poison <*enable*|*disable*>	Sets whether RIP routes on the VLAN learned from a neighbor are advertised back to the neighbor. If disabled, split horizon is invoked and IP routes learned from an immediate neighbor are not advertised back to the neighbor. If enabled, the RIP updates sent to a neighbor from which a route is learned are “poisoned” with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network.
supply <*enable*|*disable*>	Configures whether the switch supplies (talk to) the default route without advertising any other routes.
trigger <*enable*|*disable*>	Enables or disables automatic triggered updates for RIP.

Refer to Table 12 on page 214 for actions resulting from RIP supply and listen settings.

Figure 127 shows output for the **config vlan ip rip info** command.

Figure 127 config vlan ip rip info command output

```
Passport 1100# config vlan ip rip info
object <vid> = ip is out of range
object <vid> required
<vid>            = vlan id {1..4094}

vlan commands
action          vlan action
agetime         change dynamic vlan membership agetime
create          create a vlan
delete          delete a vlan
fdb-entry       forwarding database
fdb-filter      vlan bridge filter ports
fdb-static      vlan bridge static ports
highpriority    change a vlan high priority
igmp-snoop      set igmp-snoop on a vlan
info            show current level parameter settings and next level directories
ip              vlan ip commands
ipx             vlan ipx commands
name            change the name of a vlan
ports           vlan ports commands
srcmac          vlan change source mac address commands
static-mcastmac vlan static multicast mac commands
```

show vlan info rip command

The **`show vlan info rip`** command shows the RIP parameters for all VLANs or a specified VLAN.

The command syntax is:

`show vlan info rip [<vid>]`

Figure 128 shows output for the **`show vlan info rip`** command.

Figure 128 show vlan info rip command output

```
Passport 1100# show vlan info rip

================================================================================
                                    Vlan Rip
================================================================================
VLAN        ADVERTISE ACCEPT  TRIGGERED AUTOAGG
ID   ENABLE DEFAULT   DEFAULT UPDATE    ENABLE  SUPPLY LISTEN POISON
--------------------------------------------------------------------------------
1    false  false     false   false     false   true   true   false
2    false  false     false   false     false   true   true   false
45   false  false     false   false     false   true   true   false
75   false  false     false   false     false   true   true   false
76   false  false     false   false     false   true   true   false
77   false  false     false   false     false   true   true   false
78   false  false     false   false     false   true   true   false
```

OSPF commands

Routers use the Open Shortest Path First (OSPF) protocol to exchange network topology information, providing each router with a map of the network.

config ip ospf commands

The following command groups are used to configure OSPF on the switch:

- "config ip ospf command" on page 219
- "config ip ospf interface commands" on page 221
- "config ip ospf area" on page 222
- "config ip ospf area virtual-interface command" on page 224

config ip ospf command

The **config ip ospf** commands configure global OSPF parameters and use the following options:

config ip ospf followed by:	
info	Displays the current OSPF configuration on the switch (Figure 129).
admin-state <*enable*|*disable*>	Globally enables or disables the OSPF administrative status. The default is disable.
as-boundary-router <*enable*|*disable*>	Enables or disables the OSPF Autonomous System boundary router.
auto-vlink <*enable*|*disable*>	Enables or disables automatic creation of OSPF virtual links when required. The default is disable.
default-metric [ethernet <*value*>] [fast-ethernet <*value*>] [gig-ethernet <*value*>]	Sets the OSPF default metrics for: • 10 Mb/s Ethernet (default is 100). • 100 Mb/s (fast) Ethernet (default is 10). • Gigabit (gig) Ethernet (default is 1). Range is 1 to 65535.
disable	Globally disables OSPF.
enable	Globally enables OSPF.
holddown <*seconds*>	Sets the OSPF holddown timer value in seconds. The range is 3 to 60; default is 10.
router-id <*ipaddr*>	Sets the OSPF router ID IP address.
trap <*enable*|*disable*>	Enables or disables issuing traps relating to OSPF.

Figure 129 config ip ospf info command output

```
Passport 1100# config ip ospf info

Sub-Context: clear config monitor show test trace
Current Context:

                admin-state : disable
          as-boundary-router : disable
              default-metric :
                          ethernet - 100
                     fast-ethernet - 10
                      gig-ethernet - 1
                   auto-vlink : disable
                     holddown : 10
                         trap : disable
                    router_id : 22.131.38.3
                       enable : false
```

config ip ospf host-route command

Use the **config ip ospf host-route** command to configure OSPF host route parameters. The command syntax includes the IP address of the host router and the following parameters:

config ip ospf host-route <ipaddr> followed by:	
create	Creates an OSPF host route for the IP address.
delete	Deletes an OSPF host route for the IP address.
metric <*metric*>	Sets the metric (cost) for the host route (1 to 65535).

config ip ospf interface commands

The **config ip ospf interface** commands configure an OSPF interface where the interface is represented by an IP address (a.b.c.d). The commands use the following options:

config ip ospf interface <ipaddr> followed by:	
info	Displays OSPF characteristics for the interface.
admin-status <*enable*|*disable*>	Sets the state (enabled or disabled) of the OSPF interface.
area <*area*>	Sets the OSPF interface area. Use dotted-decimal notation to specify the area name. Note that the area name is not related to an IP address. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).
authentication-key <*authentication-key*>	Sets the authentication key for the OSPF interface. Specify the key in up to eight characters {string type}.
authentication-type <*auth-type*>	Sets the OSPF authentication type for the interface: none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the *interface authentication-key* command. If MD5, they must contain the md5 key.
dead-interval <*seconds*>	Sets the OSPF dead interval for the interface, the number of seconds the switch's OSPF neighbors should wait before assuming that this OSPF router is down. The range is from 1 to 2147483647. This value must be at least four times the hello interval value. The default is 40.
delete-message-digest-key <*md5-key-id*>	Deletes the specified md5 key ID from the configured md5 keys.
hello-interval <*seconds*>	Sets the OSPF hello interval for the interface, the number of seconds between hello packets sent on this interface. The range is 1 to 65535. The default is 10.
add-message-digest-key <*md5-key-id*> md5-key <*value*>	Adds an md5 key to the interface. At most two md5 keys can be configured to an interface. Multiple md5 key configurations are used for md5 transitions without bringing down an interface.
metric <*metric*>	Sets the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The range is 0 to 65535.

config ip ospf interface <ipaddr> followed by:	
poll-interval <*seconds*>	Sets the polling interval for the OSPF interface in seconds (1 to 2147483647).
priority <*priority*>	Sets the OSPF priority for the interface, during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The range is 0 to 255. The default is 1.
retransmit-interval <*seconds*>	Sets the retransmit interval for the OSPF interface, the number of seconds between link-state advertisement retransmissions (1 to 3600).
transit-delay <*seconds*>	Sets the transit delay time for the OSPF interface. the estimated time in seconds it takes to transmit a link-state update packet over the interface (1 to 3600).

config ip ospf area

The **config ip ospf area** commands control the OSPF area parameters, where <area> is the IP address of an OSPF area. Use dotted-decimal notation to specify the area name. You can use any value for the OSPF area name, for example, 1.1.1.1 or 200.200.200.200.

The **config ip ospf area** commands use the following options:

config ip ospf area <area> followed by:	
info	Displays OSPF area characteristics (Figure 130).
create	Creates an OSPF area.
delete	Deletes an OSPF area.
import-summaries <*true*|*false*>	Sets the area's support for importing summary advertisements into a stub area. This field should be used only if the area stub is set to true.
nssa <*true*|*false*>	Sets a not so stubby area (true or false). An NSSA prevents flooding of normal route advertisements into the area by replacing them with a default route.

config ip ospf area <area> followed by:	
stub <*true*|*false*>	Sets the import external option for this area to be stub or not {true|false}. A stub area has only one exit point (router interface) out of the area.
stub-metric <*stub-metric*>	Stub default metric for this stub area, which is the cost from 0 to 16777215. This is the metric value applied at the indicated type of service.

Figure 130 config ip ospf area info command output

```
Passport 1100# config ip ospf area 1.0.0.0 info

Sub-Context: clear config monitor show test trace
Current Context:

                      create : not created
                      delete : not created
            import-summaries : not created
                        nssa : not created
                        stub : not created
                 stub-metric : not created
```

config ip ospf area range commands

The **config ip ospf area range** commands control the OSPF area range parameters, where <area> is the identification of an OSPF area and <ipaddr/mask> is the IP address and subnet mask of the range.

The **config ip ospf area range** commands use the following options:

config ip ospf area <area> range <ipaddr/mask> followed by:	
create advertise-mode <*value*>lsa-type <*value*>	Creates an OSPF area range with the specified IP address and advertising mode.
delete	Deletes an OSPF area range.
info	Displays information about the OSPF area range settings.

config ip ospf area virtual-interface command

The **config ip ospf area virtual-interface** commands configure an OSPF area virtual interface. All of the commands have the following required parameters:

- *area* is the identification of an OSPF area in dotted-decimal notation. You can use any value for the OSPF area name, for example, 1.1.1.1 or 200.200.200.200.
- virtual-interface <*nbr*> is the OSPF router ID of the neighbor.

config ip ospf area <area> virtual-interface <nbr> followed by:	
info	Displays current OSPF area virtual interface information.
create	Creates a virtual interface area identifier.
delete	Deletes the virtual interface.
authentication-key <*authentication-key*>	Sets the authentication key simple password in eight characters <type string>.
authentication-type <*auth-type*>	Sets the OSPF authentication type for the OSPF area: none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the md5 key.
dead-interval <*seconds*>	Sets the dead interval for the virtual interface, which is the number of seconds that a router's hello packets have not been seen before its neighbors declare the router down (1 to 214783647). This value must be at least four times the hello interval value. The default is 60.
delete-message-digest-key <*md5-key-id*>	Deletes the specified md5 key ID from the configured md5 keys.
hello-interval <*seconds*>	Sets the hello interval for the virtual interface, which is the length of time (in seconds) between the hello packets that the router sends on the interface (1 to 65535). The default is 10.
add-message-digest-key <*md5-key-id*> md5-key <*value*>	Adds an md5 key to the interface. Two md5 keys can be configured to an interface. Multiple md5 key configurations are used for md5 transitions without bringing down an interface.

config ip ospf area <area> virtual-interface <nbr> followed by:	
retransmit-interval <*seconds*>	Sets the retransmit interval for the virtual interface, which is the number of seconds between link-state advertisement retransmissions (1 to 3600).
transit-delay <*seconds*>	Sets the transmit delay for the virtual interface, which is the estimated number of seconds it takes to transmit a link-state update over the interface (1 to 3600).

Note: Both sides of the OSPF connection must use the same authentication type and key.

show ip ospf commands

The **show ip ospf** commands are used to display the switch OSPF parameters.

show ip ospf area command

The **show ip ospf area** command displays the OSPF area parameters.

Figure 131 shows output for the **show ip ospf area** command.

Figure 131 show ip ospf area command output

```
Passport 1100# show ip ospf area

================================================================================
                                    Ospf Area
================================================================================
AREA_ID         STUB_AREA  NSSA          IMPORT_SUM ACTIVE_IFCNT
--------------------------------------------------------------------------------
0.0.0.0         false      false         true       0

STUB_COST SPF_RUNS  BDR_RTR_CNT ASBDR_RTR_CNT LSA_CNT   LSACK_SUM
--------------------------------------------------------------------------------
0         0         0           0             0         0
```

show ip ospf ase command

The **show ip ospf ase** command displays the OSPF Autonomous System External (ASE) link state advertisements. Information is displayed for all or a specified metric type.

The command syntax is:

```
show ip ospf ase [metric-type <value>] [detail]
```

Figure 132 shows output for the **show ip ospf ase** command.

Figure 132 show ip ospf ase command output

```
Passport 1100# show ip ospf ase


================================================================================
                                    Ospf AsExternal Lsas
================================================================================
```

show ip ospf default-metric command

The **show ip ospf default-metric** command displays the OSPF default metric information for each type of port.

Figure 133 shows output for the **show ip ospf default-metric** command.

Figure 133 show ip ospf default-metric command output

```
Passport 1100# show ip ospf default-metric

================================================================================
                                  Ospf Default Metric
================================================================================
  10MbpsPortDefaultMetric: 100
 100MbpsPortDefaultMetric: 10
1000MbpsPortDefaultMetric: 1
```

show ip ospf host-route command

The **show ip ospf host-route** command displays the OSPF host route configuration including host IP address, type of service, and the metric used.

show ip ospf ifstats command

The **show ip ospf ifstats** command displays IP OSPF interface statistics.

The command syntax is:

```
show ip ospf ifstats [mismatch]
```

where:

`mismatch` is the number of times the area ID is not matched.

Figure 134 shows output for the **show ip ospf ifstats** command.

Figure 134 show ip ospf ifstats command output

```
Passport 1100# show ip ospf ifstats

================================================================================
                                    Ospf Interface Statistics
================================================================================
               ---HELLOS---- ---DBS--- -LS REQ-- --LS UDP--- --LS ACK---
INTERFACE      RX     TX     RX   TX   RX   TX   RX    TX     RX    Tx
--------------------------------------------------------------------------------
192.168.30.168 0      0      0    0    0    0    0     0      0     0
```

show ip ospf info command

The **show ip ospf info** command displays the current OSPF settings for the switch.

Figure 135 shows output for the **show ip ospf info** command.

Figure 135 show ip ospf info command output

```
Passport 1100# show ip ospf info

================================================================================
                                    Ospf General
================================================================================

          RouterId: 22.131.38.3
         AdminStat: disabled
     VersionNumber: 2
  AreaBdrRtrStatus: false
    ASBdrRtrStatus: false
    ExternLsaCount: 0
 ExternLsaCksumSum: 0(0x0)
        TOSSupport: 0
  OriginateNewLsas: 0
         RxNewLsas: 0
        TrapEnable: false
AutoVirtLinkEnable: false
   SpfHoldDownTime: 10
```

show ip ospf interface command

The **show ip ospf interface** command displays information about the OSPF interface.

Figure 136 shows output for the **show ip ospf interface** command.

Figure 136 show ip ospf interface command output

```
Passport 1100# show ip ospf interface

================================================================================
                                    Ospf Interface
================================================================================
INTERFACE       AREAID          ADMINST IFST METR PRIO DR/BDR          AUTHKEY
AUTHTYPE
--------------------------------------------------------------------------------
168.192.10.168  0.0.0.0         disable Down 10   1    0.0.0.0
none
                                                       0.0.0.0
192.168.60.168  0.0.0.0         disable Down 10   1    0.0.0.0
none
                                                       0.0.0.0
10.10.40.168    0.0.0.0         disable Down 10   1    0.0.0.0
none
                                                       0.0.0.0
192.168.10.168  0.0.0.0         disable Down 10   1    0.0.0.0
none
                                                       0.0.0.0
192.168.30.168  0.0.0.0         enable  Down 10   1    0.0.0.0
none
                                                       0.0.0.0
```

show ip ospf int-timers command

The **show ip ospf int-timers** command displays the parameters for the OSPF interface timers.

Figure 137 shows output for the **show ip ospf int-timers** command.

Figure 137 show ip ospf int-timers command output

```
Passport 1100# show ip ospf int-timers

================================================================================
                                Ospf Interface Timer
================================================================================
                            TRANSIT  RETRANS  HELLO    DEAD     POLL
INTERFACE       AREAID      DELAY    INTERVAL INTERVAL INTERVAL INTERVAL
--------------------------------------------------------------------------------
168.192.10.168  0.0.0.0     1        5        10       40       120
192.168.60.168  0.0.0.0     1        5        10       40       120
10.10.40.168    0.0.0.0     1        5        10       40       120
192.168.10.168  0.0.0.0     1        5        10       40       120
192.168.30.168  0.0.0.0     1        5        10       40       120
```

show ip ospf lsdb command

The **show ip ospf lsdb** command displays the OSPF link state database table.

The command syntax is:

```
show ip ospf lsdb [area <value>] [lsatype <value>] [lsid
<value>] [adv_rtr <value>] [detail]
```

You can optionally specify an area string, link state advertisement type (0 to 5), link state ID, or advertising router. Entering [detail] provides more details.

Figure 138 shows output for the **show ip ospf lsdb** command.

Figure 138 show ip ospf lsdb command output

```
Passport 1100# show ip ospf lsdb

================================================================================
                                    Ospf Lsdb
================================================================================

================================================================================
                                    AsExternal Lsas
================================================================================
```

show ip ospf neighbors commands

The **show ip ospf neighbors** command displays OSPF neighbors with parameters.

Figure 139 shows output for the **show ip ospf neighbors** command.

Figure 139 show ospf neighbors command output

```
Passport 1100# show ip ospf neighbors

================================================================================
                                  Ospf Neighbors
================================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN
--------------------------------------------------------------------------------
```

show ip ospf range command

The **show ip ospf range** command displays the OSPF range including area ID, range network address, range subnet mask, and range flag.

Figure 140 shows output for the **show ip ospf range** command.

Figure 140 show ip ospf range command output

```
Passport 1100# show ip ospf range

================================================================================
                                    Ospf Area Range
================================================================================
AREA_ID         RANGE_NET       RANGE_MASK      RANGE_FLAG      LSDB_TYPE
--------------------------------------------------------------------------------
```

show ip ospf stats command

The **show ip ospf stats** command displays the OSPF statistics.

Figure 141 shows output for the **show ip ospf stats** command.

Figure 141 show ip ospf stats command output

```
Passport 1100# show ip ospf stats

================================================================================
                                    Ospf Statistics
================================================================================

    NumBufAlloc: 0
     NumBufFree: 0
NumBufAllocFail: 0
 NumBufFreeFail: 0
       NumTxPkt: 0
       NumRxPkt: 0
   NumTxDropPkt: 0
   NumRxDropPkt: 0
    NumRxBadPkt: 0
      NumSpfRun: 0
     LastSpfRun: 0x0
    LsdbTblSize: 0
```

configure ethernet port ip ospf commands

The port-based OSPF commands set OSPF parameters for a specific port. The parameter <ports> specifies the ports for which you are entering the command.

The command syntax is:

```
portlist {slot/port[-slot/port][, ...]}
```

The port-based OSPF commands use the following options:

config ethernet <port> ip ospf followed by:	
info	Displays OSPF characteristics on the port (Figure 142).
advertise-when-down <*enable*|*disable*>	If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. **Note:** When you configure a port without any link and enable advertise-when- down, it will not advertise your route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter should be disabled.
enable	Enables OSPF on the port.
disable	Disables OSPF on the port.
area <*ipaddr*>	Sets the OSPF identification number for the area, typically formatted as an IP address.
authentication-key <*string*>	Is the authentication key for the port (OSPF interface). Specify the key as a simple password with eight characters {string}.
authentication-type <*auth-type*>	Sets the OSPF authentication type for the port: none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the md5 key.
dead-interval <*seconds*>	Sets the router OSPF dead interval—the number of seconds the switch's OSPF neighbors should wait before assuming that the OSPF router is down. The range is 1 to 2147836437; the default is 4. The value must be at least 4 times hello interval.

config ethernet <port> ip ospf followed by:	
hello-interval <*seconds*>	Sets the OSPF hello interval, which is the number of seconds between hello packets sent on this interface. You can specify a value from 1 to 65535. The default is 1.
metric <cost>	Sets the OSPF metric associated with this interface and advertised in router link advertisements. The range is from 0 to 65535; the default is 0.
priority <integer>	Sets the OSPF priority for the port (0 to 255) during the election process for the designated router. The port with the highest priority number is the best candidate for the designated router. If you set the priority to 0, the port cannot become either the designated router or a backup designated router. The default is 1.

Note: Both sides of the OSPF connection must use the same authentication type and key.

Figure 142 config ethernet ip ospf info command output

```
Passport 1100# config ethernet ip ospf info
object <ports> = ip is out of range
object <ports> required
<ports>          = portlist {slot/port[-slot/port][,...]}

port commands
auto-negotiate  set auto-negotiate
default-vlan-id set default vlan id
duplex          set duplex
high-priority   set high priority for a port
info            show current level parameter settings and next level directories
ip              port ip commands
linktrap        set link up/down trap
lock            set lock
oversize-frame  set oversized frame
perform-tagging set perform tagging option
preferred-phy   set preferred connector to a port
speed           set speed
state           set port state up/down/test
stg             set port stg commands
tagged-frames-discardset discard tagged frames
unknown-mac-discarddiscard unknown source mac frames commands
untagged-frames-discardset discard untagged frames
```

show port ospf commands

The **show port ospf** commands display OSPF parameters and statistics for a specified port or all ports.

show ports error ospf command

The **show ports error ospf** command displays extended information about OSPF errors for a specified port or all ports.

The command syntax is:

```
show ports error ospf [<ports>]
```

Figure 143 shows output for the **show ports error ospf** command.

Figure 143 show ports error ospf command output

```
Passport 1100# show ports error ospf

================================================================================
                                    Port Ospf Error
================================================================================
PORT  VERSION  AREA     AUTHTYPE AUTH     NET_MASK HELLOINT DEADINT  OPTION
NUM   MISMATCH MISMATCH MISMATCH FAILURES MISMATCH MISMATCH MISMATCH MISMATCH
--------------------------------------------------------------------------------
3/13  0        0        0        0        0        0        0        0
3/15  0        0        0        0        0        0        0        0
```

show ports info ospf command

The **show ports info ospf** command displays information about the OSPF parameters for a specified port or all ports.

The command syntax is:

```
show ports info ospf [<ports>]
```

Figure 144 shows output for the **show ports info ospf** command.

Figure 144 show ports info ospf command output

```
Passport 1100# show ports info ospf

================================================================================
                                    Port Ospf
================================================================================
PORT         HELLO   RTRDEAD OSPF
NUM   ENABLE INTVAL  INTVAL  PRIORITY METRIC AUTHTYPE AUTHKEY    AREA_ID
--------------------------------------------------------------------------------
3/1   true   10      40      1        0      none               0.0.0.0
3/2   false  10      40      1        0      none               0.0.0.0
3/3   true   10      40      1        0      none               0.0.0.0
3/4   true   10      40      1        0      none               0.0.0.0
3/5   true   10      40      1        0      none               0.0.0.0
3/6   true   10      40      1        0      none               0.0.0.0
3/7   true   10      40      1        0      none               0.0.0.0
3/8   true   10      40      1        0      none               0.0.0.0
3/9   true   10      40      1        0      none               0.0.0.0
3/10  true   10      40      1        0      none               0.0.0.0
3/11  true   10      40      1        0      none               0.0.0.0
3/12  true   10      40      1        0      none               0.0.0.0
3/13  true   10      40      1        10     none               0.0.0.0
3/14  false  10      40      1        0      none               0.0.0.0
3/15  false  10      40      1        10     none               0.0.0.0
3/16  true   10      40      1        0      none               0.0.0.0
```

show ports stats ospf main command

The **`show ports stats ospf main`** command displays basic OSPF information about a specified port or all ports.

The command syntax is:

`show ports stats ospf main [<`*`ports`*`>]`

Figure 145 shows output for the **`show ports stats ospf main`** command.

Figure 145 show ports stats ospf main command output

```
Passport 1100# show ports stats ospf main

================================================================================
                                    Port Stats Ospf
================================================================================
PORT_NUM RX_HELLO   TX_HELLO   RXDB_DESCR TXDB_DESCR RXLS_UPDATE   TXLS_UPDATE
--------------------------------------------------------------------------------
3/1      0          0          0          0          0             0
3/3      0          0          0          0          0             0
3/4      0          0          0          0          0             0
3/5      0          0          0          0          0             0
3/6      0          0          0          0          0             0
3/7      0          0          0          0          0             0
3/8      0          0          0          0          0             0
3/9      0          0          0          0          0             0
3/10     0          0          0          0          0             0
3/11     0          0          0          0          0             0
3/12     0          0          0          0          0             0
3/13     0          0          0          0          0             0
3/14     0          0          0          0          0             0
3/16     0          0          0          0          0             0
```

show ports stats ospf extended command

The **show ports stats ospf extended** command displays extended OSPF information about all or specified ports.

The command syntax is:

```
show ports stats interface extended [<ports>]
```

Figure 146 shows output for the **show ports stats ospf extended** command.

Figure 146 show ports stats ospf extended command output

```
Passport 1100# show ports stats ospf extended

================================================================================
                                    Port Stats Ospf Extended
================================================================================
PORT_NUM RXLS_REQS   TXLS_REQS   RXLS_ACKS   TXLS_ACKS
--------------------------------------------------------------------------------
3/1      0           0           0           0
3/3      0           0           0           0
3/4      0           0           0           0
3/5      0           0           0           0
3/6      0           0           0           0
3/7      0           0           0           0
3/8      0           0           0           0
3/9      0           0           0           0
3/10     0           0           0           0
3/11     0           0           0           0
3/12     0           0           0           0
3/13     0           0           0           0
3/14     0           0           0           0
3/16     0           0           0           0
```

config vlan ip ospf commands

The **`config vlan ip ospf`** commands set OSPF parameters for the specified VLAN (vid range is 1 to 4095). The commands use the following options:

`config vlan <vid> ip ospf` followed by:	
`info`	Displays OSPF characteristics on the VLAN (Figure 147).
`advertise-when-down <enable|disable>`	If enabled, the network on this interface is advertised as up, even if no ports in the VLAN are active. The default is disabled. **Note**: When you create a VLAN with no active ports and enable advertise-when- down, it will not advertise your route until a port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, disable this parameter.
`enable`	Enables OSPF on the VLAN.
`disable`	Disables OSPF on the VLAN.
`area <ipaddr>`	The OSPF interface area ID for the VLAN, and the IP address of the VLAN OSPF area.

config vlan <vid> ip ospf followed by:	
`authentication-key <string>`	Sets the authorization key for the VLAN. Specify the key in up to eight characters {string type}.
`authentication-type <auth-type>`	Sets the OSPF authentication type for the VLAN: none, simple password, or MD5 authentication. If simple, all OSPF updates received by the VLAN must contain the authentication key specified by the `area authentication-key` command. If MD5, they must contain the md5 key.
`dead-interval <seconds>`	Sets the OSPF dead interval for the VLAN, the number of seconds the switch's OSPF neighbors should wait before assuming that this OSPF router is down. The range is from 1 to 2147483647. This value must be at least four times the hello interval value. The default is 40.
`hello-interval <seconds>`	Sets the OSPF hello interval for the VLAN, which is the number of seconds between hello packets sent on this VLAN. The range is 1 to 65535. The default is 10.
`metric <cost>`	Sets the OSPF metric for the VLAN. The switch advertises the metric in router link advertisements. The range is 0 to 65535. The default is 0.
`priority <integer>`	Sets the OSPF priority for the VLAN, during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If the priority is 0, the VLAN cannot become the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The range is 0 to 255. The default is 1.

Note: Both sides of the OSPF connection must use the same authentication type and key.

Figure 147 config vlan ip ospf info command output

```
Passport 1100# config vlan 1 ip ospf info

Sub-Context: clear config monitor show test trace
Current Context:

          advertise-when-down : disable
                        ospf : disable
             hello-interval : 10
              dead-interval : 40
                   priority : 1
                     metric : 10
          authentication-type : none
           authentication-key :
                        area : 0.0.0.0
```

show vlan info ospf command

The **show vlan info ospf** command shows the OSPF parameters configured for all or a specified VLAN.

The command syntax is:

`show vlan info ospf [<vid>]`

Figure 148 shows output for the **show vlan info ospf** command.

Figure 148 show vlan info ospf command output

```
Passport 1100# show vlan info ospf

================================================================================
                                    Vlan Ospf
================================================================================
VLAN        HELLO    RTRDEAD  DESIGRTR
ID  ENABLE INTERVAL INTERVAL PRIORITY METRIC AUTHTYPE AUTHKEY    AREAID
--------------------------------------------------------------------------------
1   false  10       40       1        10     none              0.0.0.0
2   false  10       40       1        0      none              0.0.0.0
45  false  10       40       1        10     none              0.0.0.0
75  false  10       40       1        0      none              0.0.0.0
76  false  10       40       1        0      none              0.0.0.0
77  false  10       40       1        0      none              0.0.0.0
78  false  10       40       1        10     none              0.0.0.0
```

VRRP commands

The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate a failure in the static default routed environment by using a logical IP address, which is shared between two or more routers connecting the subnet to the enterprise network. VRRP parameters are set on an isolated routing port or on a VLAN.

Note: In -A (ARU2) hardware, four VRRP interfaces (isolated routing ports or VLANs) are allowed per switch and all virtual router IDs must be unique. In -B (ARU3) hardware, a maximum of 255 VRIDs can be configured.

config ip vrrp commands

Use the **config ethernet*<ports>* ip vrrp *<vrid>* holddown-timer *<seconds>*** command to configure the delay timer. Use the **config vlan*<vid>* ip vrrp *<vrid>* holddown-timer *<seconds>*** command to configure the VLANs. You may enter from 0 to 21600 seconds.

You can monitor the main or extended VRRP statistics using the **monitor ports stats vrrp extended *<ports>*** or the **monitor ports stats vrrp main *<ports>*** commands. You can also show the statistics in either mode by using the **show ports stats vrrp extended *[<ports>]*** command, or the **show ports stats vrrp main *[<ports>]*** command.

To manually override the delay timer and force preemption for a port using the CLI, use the **config ethernet <port> ip vrrp <vrid> action <none|preemptHoldDownTimer>** command. To force preemption for a VLAN, use the **config vlan <vid> ip vrrp <vrid> action <none|preemptHoldDownTimer>** command.

The **config ip vrrp** commands use the following options:

config ip vrrp followed by:	
info	Displays whether global send trap or ping are enabled or disabled.
ping-virtual-address <*enable*|*disable*>	Enables all interfaces to respond to virtual IP pings.
send-trap <*enable*|*disable*>	Enables all interfaces to send traps.

config ethernet port ip vrrp commands

The **config ethernet port ip vrrp** command sets VRRP on a port and uses the following options:

config ethernet <ports> ip vrrp <vrid> followed by:	
info	Displays the current port VRRP configuration (Figure 149).
action <action choice>	Bypasses hold down timer.
address <*ipaddr*>	Sets the IP address of the virtual router interface.
adver-int <*seconds*>	Sets the advertising interval (in seconds), which is the time interval between sending advertisement messages. The value must be the same on all participating routers. The range is 1 to 255, and the default is 1.
critical-ip <*ipaddr*>	Sets the critical IP address for VRRP. This address is an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface went down).
delete	Deletes the VRRP from the port.
disable	Disables the VRRP on the port.
enable	Enables VRRP on the port.

config ethernet <ports> ip vrrp <vrid> followed by:	
holddown-timer <seconds>	Sets hold down timer.
priority <*prio*>	Sets the port VRRP priority (1 to 254) value to be used by this VRRP router. The default is 100. The value 255 is assigned to the router that owns the IP address associated with the virtual router.

Figure 149 config ethernet ports ip vrrp info command output

```
Passport 1100# config ethernet 3/3 ip vrrp info
object <vrid> = info is out of range
object <vrid> required
<vrid>           = virtual router id {1..255}

vrrp configuration commands
address          set vrrp ip address
adver-int        set vrrp advertisment interval
critical-ip      set vrrp critical ip address
delete           delete vrrp
disable          disable vrrp
enable           enable vrrp
holddown-timer   set vrrp holddown timer
info             show current level parameter settings and next level directories
priority         set vrrp priority
```

show port vrrp commands

The **show port vrrp** commands display port VRRP configuration and statistics.

show ports info vrrp main command

The **show ports info vrrp main** command displays basic VRRP configuration information about a specified port or all ports.

The command syntax is:

show ports info vrrp main [<*ports*>]

Figure 150 shows output for the **show ports info vrrp main** command.

Figure 150 show ports info vrrp main command output

```
Passport 1100# show ports info vrrp main

================================================================================
                                    Port Vrrp
================================================================================
PORT_NUM VRRP_ID IP_ADDRESS      VIRTUAL_MAC_ADDR
--------------------------------------------------------------------------------
```

show ports info vrrp extended command

The **show ports info vrrp extended** command displays extended VRRP configuration information about a specified port or all ports.

The command syntax is:

```
show ports info vrrp extended [<ports>]
```

Figure 151 shows output for the **show ports info vrrp extended** command. The Master_IPaddr is the IP address of the master router.

Figure 151 show ports info vrrp extended command output

```
Passport 1100# show ports info vrrp extended

================================================================================
                                 Port Vrrp Extended
================================================================================
PORT  STATE      CONTROL  PRIORITY  MASTER_IPADDR   ADVERTISE CRITICAL_IPADDR
--------------------------------------------------------------------------------
```

show ports stats vrrp command

The **show ports stats vrrp** command displays VRRP information about a specified port or all ports.

The command syntax is:

```
show ports stats vrrp [<ports>]
```

config vlan ip vrrp commands

The **vlan vrrp** commands set VRRP on a VLAN using required parameters.

The command syntax is:

```
config vlan <vid> ip vrrp <vrid>
```

where:

vid is the VLAN ID (1 to 4095).

vrid is the virtual router ID (1 to 255), a number that uniquely identifies a virtual router on a given VRRP router. The virtual router acts as the default router for one or more assigned addresses.

The **vlan vrrp** commands use the following options:

config vlan <vid> ip vrrp <vrid> followed by:	
action <action choice>	Bypasses the hold down timer.
info	Displays the current VLAN VRRP settings.
address <*ipaddr*>	Sets the IP address of the virtual router interface.
adver-int <*seconds*>	Sets the advertising interval (in seconds), which is the time interval between sending advertisement messages. The range is 1 to 255, and the default is 1.
critical-ip <*ipaddr*>	Sets the critical IP address for VRRP. The address is an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface goes down.
delete	Deletes the VRRP on the VLAN.
disable	Disables the VRRP on the VLAN.
enable	Enables the VRRP on the VLAN.
holddown-timer <seconds>	Sets hold down timer.
priority <*prio*>	Sets the port VRRP priority (1 to 254) value to be used by this VRRP router. The default is 100. The value 255 is assigned to the router that owns the IP address associated with the virtual router.

show vlan vrrp commands

Two show commands display VLAN VRRP information.

show vlan info vrrp main command

The **show vlan info vrrp main** command displays the basic VRRP configuration for a specified VLAN or for all VLANs.

The command syntax is:

```
show vlan info vrrp main [<vid>]
```

show vlan info vrr extended command

The **show vlan info vrr extended** command displays the extended VRRP configuration for a specified VLAN or for all VLANs.

The command syntax is:

```
show vlan info vrrp extended [<vid>]
```

show ip vrrp commands

The **show ip vrrp** commands display information about VRRP as configured on the switch.

show ip vrrp info command

The **show ip vrrp info** command displays VRRP information for the interface. If a virtual router ID or IP address is entered, the information is displayed only for that VRID or interface. If a virtual router ID or IP address is not entered, all VRRP interfaces are listed.

The command syntax is:

```
show ip vrrp info [<vrid>] [ipaddr]
```

show ip vrrp stats command

The **show ip vrrp stats** command displays counter information for a specified VRRP or for all VRRP interfaces. You must enter a VRID (virtual router ID). If an IP address is entered, the information is displayed only for that interface. If you do not enter an IP address, all VRRP interfaces are listed.

The command syntax is:

```
show ip vrrp stats <vrid> [ipaddr]
```

IP multicast commands

Caution: Nortel Networks does not recommend or support IP Multicast with IGMP or DVMRP on the Passport 1000 platform.

The **IP multicast** commands allow you to configure and view IP multicasting parameters.

config ip mroute commands

The **config ip mroute** commands configure multicast routing and use the following options:

config ip mroute followed by:	
`info`	Displays information about the multicast route.
`interface <ipaddr> info`	Displays information about the multicast route interface.
`mroute interface <ipaddr> ttl <ttl>`	Sets the default time-to-live threshold for the multicast route interface.

show ip mroute commands

The **show ip mroute** commands display information about the multicast route set up on the switch.

show ip mroute interface command

The **show ip mroute interface** command displays information about the multicast interface.

Figure 152 shows output for the **show ip mroute interface** command.

Figure 152 show ip mroute interface command output

```
swlab-edge2# show ip mroute interface

================================================================================
                                        Mroute Interface
================================================================================
INTERFACE  TTL   PROTOCOL
--------------------------------------------------------------------------------
Port2/1    1     dvmrp
Port2/2    1     dvmrp
Vlan1      1     dvmrp
```

show ip mroute next-hop command

The **show ip mroute next-hop** command displays information about the next hop for the multicast route.

Figure 153 shows output for the **show ip mroute next-hop** command.

Figure 153 show ip mroute next-hop command output

```
Passport 1200# show ip mroute next-hop

================================================================================
                                    Mroute Next Hop
================================================================================
INTERFACE  GROUP           SOURCE          SRCMASK         ADDRESS
--------------------------------------------------------------------------------
INTERFACE  STATE      EXPIRY_TIME     CLOSE_HOP       PROTOCOL
--------------------------------------------------------------------------------
Total 0
```

show ip mroute route

The **show ip mroute route** command displays information about the multicast route.

Figure 154 shows output for the **show ip mroute route** command.

Figure 154 show ip mroute route command output

```
Passport 1200# show ip mroute route

================================================================================
                                    Mroute Route
================================================================================
GROUP           SOURCE          SRCMASK         UPSTREAM_NBR    IF    EXPIR PROT
--------------------------------------------------------------------------------
Total 0
```

show ports stats routing command

The **show ports stats routing** command displays routing information about a specified port or for all ports.

The command syntax is:

`show ports stats routing [<ports>]`

Figure 155 shows output for the **show ports stats routing** command.

Figure 155 show ports stats routing command output

```
Passport 1200# show ports stats routing

================================================================================
                                    Port Stats Routing
================================================================================
PORT      IN_FRAME    IN_FRAME    IN          OUT_FRAME   OUT_FRAME
NUM       UNICAST     MULTICAST   DISCARD     UNICAST     MULTICAST
--------------------------------------------------------------------------------
1/1       5489        0           1           0           0
1/2       0           0           0           0           0
1/3       0           0           0           0           0
1/4       0           0           0           0           0
1/5       0           0           0           0           0
1/6       0           0           0           0           0
1/7       0           0           0           0           0
1/8       0           0           0           0           0
1/9       0           0           0           0           0
1/10      0           0           0           0           0
1/11      0           0           0           0           0
1/12      0           0           0           0           0
1/13      0           0           0           0           0
1/14      0           0           0           0           0
1/15      0           0           0           0           0
1/16      0           0           0           0           0
```

DVMRP commands

Caution: Nortel Networks does not recommend or support IP Multicast with IGMP or DVMRP on the Passport 1000 platform.

Distance Vector Multicast Routing Protocol (DVMRP) is used between routers to exchange multicast routing information. The protocol can be configured on an isolated routing port or on a VLAN. It must be enabled globally in order to take effect.

config ip dvmrp commands

The **`config ip dvmrp`** commands are global DVMRP commands.

config ip dvmrp command

The **config ip dvmrp** commands use the following options:

config ip dvmrp followed by:	
info	Displays DVMRP settings (Figure 156).
disable	Globally disables DVMRP.
enable	Globally enables DVMRP.
update-interval <*integer*>	Sets the time interval (in seconds) between DVMRP router update messages. The range is 10 to 2000; the default is 60.
triggered-update-interval <*integer*>	Sets the time interval (in seconds) between triggered update messages sent when routing information changes. The range is 5 to 1000; the default is 5.
leaf-timeout <*integer*>	Sets the length of time (in seconds) the router waits for a response from a neighbor before considering the attached network to be a leaf network. The range is 25 to 4000; the default is 200.
nbr-timeout <*integer*>	Sets the length of time (in seconds) the router waits to receive a report from a neighbor before considering the connection inactive. The range is 35 to 8000; the default is 35.
nbr-probe-interval <*integer*>	Determines how often the DVMRP router sends neighbor probe messages on its interface. The range is 5 to 30 seconds; the default is 10.

Figure 156 config ip dvmrp info command output

```
Passport 1200# config ip dvmrp info

Sub-Context: clear config monitor show test trace
Current Context:

                        enable : false
                update-interval : 60
     triggered-update-interval : 5
                   leaf-timeout : 200
                    nbr-timeout : 35
           nbr-probe-interval : 10
```

config ip dvmrp interface command

The **config ip dvmrp interface** commands require an IP address and use the following options:

config ip dvmrp interface <ipaddr> **followed by:**	
disable	Disables DVMRP on the local router interface.
enable	Enables DVMRP on the local router interface.
info	Displays information about the specified DVMRP local router interface.
metric <*cost*>	Sets the cost metric (maximum number of hops) for the router interface. The range is 1 to 31.

show ip dvmrp commands

The **show ip dvmrp** commands display information about the DVMRP as set on the switch.

show ip dvmrp info command

The **show ip dvmrp** command displays information about the general DVMRP group.

Figure 157 shows output for the **show ip dvmrp** command.

Figure 157 show ip dvmrp info command output

```
Passport 1200# show ip dvmrp info

================================================================================
                                    Dvmrp General Group
================================================================================
AdminStat               : disabled
Genid                   : 0
Version                 : (null)
NumRoutes               : 0
NumReachableRoutes      : 0

UpdateInterval          : 60
TriggeredUpdateInterval : 5
LeafTimeOut             : 200
NbrTimeOut              : 35
NbrProbeInterval        : 10
```

show ip dvmrp interface command

The **`show ip dvmrp interface`** command displays information about the DVMRP interface set up on the switch.

Figure 158 shows output for the **`show ip dvmrp interface`** command.

Figure 158 show ip dvmrp interface command

```
Passport 1200# show ip dvmrp interface

================================================================================
                                    Dvmrp Interface
================================================================================
IF        ADDR            METRIC     OPERSTAT
--------------------------------------------------------------------------------
Port2/1   192.168.50.170  1          down
Port2/2   192.168.40.170  1          down
Vlan1     10.10.40.170    1          down
```

show ip dvmrp neighbor command

The **`show ip dvmrp neighbor`** command displays information about the configured DVMRP neighbor.

Figure 159 shows output for the **`show ip dvmrp neighbor`** command.

Figure 159 show ip dvmrp neighbor command output

```
swlab-edge2# show ip dvmrp neighbor

================================================================================
                                    Dvmrp Neighbor
================================================================================
INTF    ADDRESS         EXPIRE GENID       MAJ/MIN CAPABILITY    STATE    UPTIME
                                           VERSION
--------------------------------------------------------------------------------
Port2/2 192.168.40.209  30     980819675   3/255   prune,genID   active 40:15:28

Total 1
```

show ip dvmrp next-hop command

The **show ip dvmrp next-hop** command shows information about the DVMRP next hop.

Figure 160 shows output for the **show ip dvmrp next-hop** command.

Figure 160 show ip dvmrp next-hop command output

```
swlab-edge2# show ip dvmrp next-hop

================================================================================
                                    Dvmrp Next Hop
================================================================================
SOURCE          MASK            INTERFACE  TYPE
--------------------------------------------------------------------------------
192.168.20.0    255.255.255.0   Port2/2    branch
192.168.30.0    255.255.255.0   Port2/1    leaf
192.168.40.0    255.255.255.0   Port2/1    leaf
192.168.50.0    255.255.255.0   Port2/1    leaf
Total 4
```

show ip dvmrp route command

The **show ip dvmrp route** command displays information about the DVMRP route.

Figure 161 shows output for the **show ip dvmrp route** command.

Figure 161 show ip dvmrp route command output

```
swlab-edge2# show ip dvmrp route

================================================================================
                                  Dvmrp Route
================================================================================
SOURCE          MASK            UPSTREAM_NBR    INTERFACE  METRIC EXPIRE
--------------------------------------------------------------------------------
192.168.20.0    255.255.255.0   0.0.0.0         Port2/1    1      215
192.168.30.0    255.255.255.0   192.168.40.209  Port2/2    2      220
192.168.40.0    255.255.255.0   0.0.0.0         Port2/2    1      160
192.168.50.0    255.255.255.0   192.168.40.209  Port2/2    3      220
Total 4
```

config ethernet ip dvmrp commands

The **`config ethernet ip dvmrp`** commands configure DVMRP at the port level. DVMRP must be enabled globally for these settings to take effect.

The DVMRP port commands require the parameter <*ports*> as the port or list of ports for the command `{slot/port[-slot/port][, ...]}` and use the following options:

`config ethernet <ports> ip dvmrp` followed by:	
`info`	Displays DVMRP settings on the port (Figure 162).
`enable`	Enables DVMRP on the port.
`disable`	Disables DVMRP on the port.
`metric <cost>`	Sets the DVMRP route metric, where the cost is the maximum number of hops with a value of 1 to 31.

Figure 162 config ethernet ip dvmrp info command output

```
Passport 1200# config ethernet 1/1 ip dvmrp info

Sub-Context: clear config monitor show test trace
Current Context:

                      dvmrp : disable
                     metric : 1
```

show ports info dvmrp command

The **show ports info dvmrp** command displays information about DVMRP configuration for a specified port or for all ports.

The command syntax is:

```
show ports info dvmrp [<ports>]
```

Figure 163 shows output for the **show ports info dvmrp** command.

Figure 163 show ports info dvmrp command output

```
Passport 1200# show ports info dvmrp

================================================================================
                                    Port Ip Dvmrp
================================================================================
PORT-NUM        DVMRP-ENABLE    METRIC
--------------------------------------------------------------------------------
1/1             disable         1
1/2             disable         1
1/3             disable         1
1/4             disable         1
1/5             disable         1
1/6             disable         1
1/7             disable         1
1/8             disable         1
1/9             disable         1
1/10            disable         1
1/11            disable         1
1/12            disable         1
1/13            disable         1
1/14            disable         1
1/15            disable         1
1/16            disable         1
2/1             disable         1
```

config vlan ip dvmrp commands

The **config vlan ip dvmrp** commands configure DVMRP on the VLAN (with a vid from 1 to 4095) and use the following options:

config vlan <vid> ip dvmrp followed by:	
info	Displays DVMRP settings on the VLAN (Figure 164).
enable	Enables DVMRP on the VLAN.
disable	Disables DVMRP on the VLAN.
metric <*cost*>	Sets the DVMRP route metric, where the cost is the maximum number of hops with a value of 1 to 31.

Figure 164 config vlan ip dvmrp info command output

```
Passport 1200# config vlan 1 ip dvmrp info

Sub-Context: clear config monitor show test trace
Current Context:

                        dvmrp : disable
                       metric : 1
```

show vlan info dvmrp command

The **show vlan info dvmrp** command displays the DVMRP configuration for a specified VLAN or for all VLANs.

The command syntax is:

```
show vlan info dvmrp [<vid>]
```

Figure 165 shows output for the **show vlan info dvmrp** command.

Figure 165 show vlan info dvmrp command output

```
Passport 1200# show vlan info dvmrp

================================================================================
                                    Vlan Ip Dvmrp
================================================================================
VLAN-ID         DVMRP-ENABLE    METRIC
--------------------------------------------------------------------------------
1               disable         1
```

Layer 3 IGMP commands

The Internet Group Management Protocol (IGMP) is used by hosts to report multicast group memberships to neighbor multicast routers. DVMRP multicasting must be enabled globally for these commands to take effect. IGMP configuration is on a per interface basis. Some features of layer 3 IGMP commands require -B hardware (ARU3).

config ip l3 igmp commands

The **`config ip l3 igmp`** commands are the interface layer 3 IGMP commands for the switch. The **`config ip l3-igmp info`** command (not shown) displays information about the current global layer 3 IGMP configuration.

config ip l3-igmp interface

The **`config ip l3-igmp interface`** commands configure the interface IP address (<*ipaddr*>) and use the following options:

`config ip l3-igmp interface <ipaddr>` followed by:	
`info`	Displays the settings of the IGMP interface.
`last-memb-query-int` <*seconds*>	Sets the length of time (in seconds) an entry remains in the multicast table before timeout. The range is 1 to 255 with a default value of 1.
`query-interval` <*seconds*>	Sets the frequency (in seconds) at which host query packets are transmitted on the interface. The range is 1 to 65535 with a default of 125.

config ip l3-igmp interface <ipaddr> followed by:	
query-max-resp <*integer*>	Sets the maximum response time (in seconds) advertised in IGMPv2 queries on the interface. Smaller values allow a router to prune groups faster. The range is 1 to 255 with a default of 10.
robustval <*integer*>	Allows tuning for the expected packet loss of a network. The range is 2 to 255 with a default of 2. Increase the value if the network has a high loss rate.
version <*integer*>	Sets the version (1 or 2) of IGMP that is running on the interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is IGMPv1 for -A modules and IGMPv2 for -B modules.

show ip l3 igmp commands

The **show ip l3 igmp** commands display information about IGMP on the switch.

show ip l3-igmp cache command

The **show ip l3-igmp cache** command displays information about the layer 3 IGMP cache.

Figure 166 shows output for the **show ip l3-igmp cache** command.

Figure 166 show ip l3-igmp cache command output

```
swlab-edge2# show ip l3-igmp cache

================================================================================
                                    Igmp Cache
================================================================================
GRPADDR         INTERFACE  LASTREPORTER    EXPIRATION V1HOSTTIMER
--------------------------------------------------------------------------------
239.255.207.31  Port2/1    192.168.20.2    259        260
239.255.214.171 Port2/1    192.168.20.2    257        255
```

show ip l3-igmp group command

The **show ip l3-igmp group** command displays information for the layer 3 IGMP group.

Figure 167 shows output for the **show ip l3-igmp group** command.

Figure 167 show ip l3-igmp group command output

```
swlab-edge2# show ip l3-igmp group

================================================================================
                                    Igmp Group
================================================================================
GRPADDR         INPORT     MEMBER          EXPIRATION
--------------------------------------------------------------------------------
239.255.207.31  2/1        192.168.20.2    259
239.255.214.171 2/1        192.168.20.2    259
```

show ip l3-igmp interface

The **show ip l3-igmp interface** command displays information for the interfaces on which layer 3 IGMP is enabled.

Figure 168 shows output for the **show ip l3-igmp interface** command.

Figure 168 show ip l3-igmp interface command output

```
Passport 1200# show ip l3-igmp interface

================================================================================
                                Igmp Interface
================================================================================
       QUERY              OPER                 QUERY   WRONG            LASTMEM
IF     INTVL STATUS VERS. VERS QUERIER         MAXRSPT QUERY JOINS ROBUST QUERY
--------------------------------------------------------------------------------
P2/1   125   inact  2     2    0.0.0.0         10      0     0     2      1
P2/2   125   inact  2     2    0.0.0.0         10      0     0     2      1
V1     125   inac
t 2     2    0.0.0.0         10      0     0     2      1
```

config ethernet ip l3-igmp commands

The **config ethernet ip l3-igmp** commands configure layer 3 IGMP on specified ports. The commands require the parameter *ports* as the port or list of ports {slot/port[-slot/port][, ...]}, and use the following options:

config ethernet <ports> ip l3-igmp followed by:	
info	Displays IGMP settings on the port (Figure 169).
last-memb-query-int <*seconds*>	Sets the length of time (in seconds) an entry remains in the multicast table before timeout. Range is 1 to 255 with a default value of 1.
query-interval <*seconds*>	Sets the frequency (in seconds) at which host query packets are transmitted on the port. The range is 1 to 65535 with a default of 125.
query-max-resp <*seconds*>	Sets the maximum response time (in seconds) advertised in IGMPv2 queries on the port. Smaller values allow a router to prune groups faster. The range is 1 to 255 with a default of 10.
robustval <*integer*>	Allows tuning for the expected packet loss of a network. The range is 2 to 255 with a default of 2. Increase the value if you expect the network to have a high loss rate.
version <*integer*>	Sets the version (1 or 2) of IGMP that is running on the port. For IGMP to function correctly, all routers on a LAN must use the same version. The default is IGMPv2 for -B hardware and IGMPv1 for -A hardware.

Figure 169 config ethernet ip l3-igmp info command output

```
Passport 1200# config ethernet 1/1 ip l3-igmp info

Sub-Context: clear config monitor show test trace
Current Context:

         last-memb-query-int : 1
              query-interval : 125
              query-max-resp : 10
                   robustval : 2
                     version : 2
```

show ports info l3-igmp command

The **show ports info l3-igmp** command displays IGMP information about a specified port or for all ports.

The command syntax is:

```
show ports info igmp [<ports>]
```

Figure 170 shows output for the **show ports info l3-igmp** command.

Figure 170 show ports info 13-igmp command output

```
Passport 1200# show ports info l3-igmp

================================================================================
                                    Port Ip Igmp
================================================================================
PORT_NUM QUERY_INTERVAL  QUERY_MAX_RESP  ROBUST     VERSION    LSTMEMBER_QUERY
--------------------------------------------------------------------------------
1/1      125             10              2          version2   1
1/2      125             10              2          version2   1
1/3      125             10              2          version2   1
1/4      125             10              2          version2   1
1/5      125             10              2          version2   1
1/6      125             10              2          version2   1
1/7      125             10              2          version2   1
1/8      125             10              2          version2   1
1/9      125             10              2          version2   1
1/10     125             10              2          version2   1
1/11     125             10              2          version2   1
1/12     125             10              2          version2   1
1/13     125             10              2          version2   1
1/14     125             10              2          version2   1
1/15     125             10              2          version2   1
1/16     125             10              2          version2   1
2/1      125             10              2          version2   1
```

config vlan ip l3-igmp commands

The **config vlan ip l3-igmp** commands configure layer 3 IGMP on a VLAN, where the VLAN ID is from 1 to 4095.

The commands use the following options:

config vlan <vid> ip l3-igmp followed by:	
`info`	Displays IGMP settings on the VLAN (Figure 171).
`last-memb-query-int <seconds>`	Sets the length of time (in seconds) an entry remains in the multicast table before timeout. Range is 1 to 255 with a default value of 1.
`query-interval <seconds>`	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. The range is 1 to 65535 with a default of 125.
`query-max-resp <seconds>`	Sets the maximum response time (in seconds) advertised in IGMPv2 queries on the VLAN. Smaller values allow a router to prune groups faster. The range is 1 to 255 with a default of 10.
`robustval <integer>`	Allows tuning for the expected packet loss of a network. The range is 2 to 255 with a default of 2. Increase the value if the network has a high loss rate.
`version <integer>`	Sets the version (1 or 2) of IGMP that is running on the VLAN. For IGMP to function correctly, all routers on a LAN must use the same version. The default is IGMPv2 for -B hardware and IGMPv1 for -A hardware.

Figure 171 config vlan ip l3-igmp info command output

```
Passport 1200# config vlan 1 ip l3-igmp info

 Sub-Context: clear config monitor show test trace
 Current Context:

          last-memb-query-int : 1
               query-interval : 125
               query-max-resp : 10
                    robustval : 2
                      version : 2
```

show vlan info l3-igmp command

The **show vlan info l3-igmp** command displays the IGMP configuration for a specified VLAN or for all VLANs.

The command syntax is:

```
show vlan info igmp [<vid>]
```

Figure 172 shows output for the **show vlan info l3-igmp** command.

Figure 172 show vlan info l3-igmp command output

```
Passport 1200# show vlan info l3-igmp

================================================================================
                                    Vlan Ip Igmp
================================================================================
VLAN_ID  QUERY_INTERVAL  QUERY_MAX_RESP  ROBUST     VERSION    LSTMEMBER_QUERY
--------------------------------------------------------------------------------
1        125             10              2          version2   1
```

IPX commands

This section provides information about using the Passport CLI for configuring and displaying the Internet Packet Exchange (IPX) protocol, the Novell Inc. adaptation of the Xerox Network System (XNS) protocol.

The Passport implementation of IPX supports four Ethernet frame formats:

- Ethernet II (ipxEthernet2)
- 802.2-LLC (ipx802dot2)
- 802.3-RAW (ipx802dot3)
- 802.3-SNAP (ipxSnap)

In addition to the IPX configuration commands, there are also commands for IPX RIP and IPX SAP.

config ipx commands

The IPX commands allow you to configure an IPX interface on the switch.

To configure an IPX interface:

1. Create a protocol-based VLAN, using one of the four supported Ethernet frame formats.

   `config vlan <vid> create byprotocol <sid> <ipx802dot3|ipx802dot2|ipxSnap|ipxEthernet2> [name <value>]`

   where:

   `vid` is the VLAN ID (2 to 4095).

   `sid` is the spanning tree ID (1 to 25).

   `protocol` is one of the four listed above.

   `name <value>` is the name of the VLAN (for example, IPX).

Note: You can also create a port-based VLAN in IPX. The procedure is the same as for a protocol-based VLAN except that you do not need to assign an encapsulation method when you create the VLAN. Use the command:

`config vlan <vid> create byport <sid> [name <value>]`

2. Remove the ports that you do not want to be part of the interface:

   `config vlan <vid> ports remove <ports> [member <value>]`

   where:

   `vid` is the VLAN created in step 1.

   `member <value>` is the slot and port number to be removed from the interface (for example, 1/5-1/16).

3. Add the ports you want to be part of the interface:

   `config vlan <vid> ports add <ports> [member <value>]`

   where:

   `vid` is the VLAN created in step 1.

`member <value>` is the slot and port number to be added to the interface (for example, 1/1-1/4).

4 Create an IPX network interface with the specified VLAN ID and encapsulation method.

```
config vlan <vid> ipx create <IPX-network-number>
[<encapsulation>]
```

where:

vid is the VLAN created in step 1.

`encapsulation` is ethernet-ii, snap, llc, or raw.

Note: The encapsulation method must be the same as the protocol selected in step 1.

5 Globally enable IPX routing on all IPX interfaces:

```
config ipx forwarding enable
```

The **`config ipx`** commands use the following options:

`config ipx` followed by:	
`info`	Displays the switch IPX configuration (Figure 173).
`forwarding info`	Indicates whether IPX is enabled or disabled on the switch and lists the IPX networks that are enabled or disabled (Figure 174).
`forwarding disable [<IPX-network-number>]`	Disables IPX forwarding globally or on a specified IPX network.
`forwarding enable [<IPX-network-number>]`	Enables IPX forwarding globally or on a specified IPX network.

Figure 173 config ipx info command output

```
Passport 1200# config ipx info

Sub-Context: clear config monitor show test trace
Current Context:

              create :
              delete : N/A
```

Figure 174 config ipx forwarding info command output

```
Passport 1200# config ipx forwarding info

Sub-Context: clear config monitor show test trace
Current Context:

          forwarding : disable

              enable :

             disable :
```

config vlan ipx commands

The **`config vlan ipx`** commands configure IPX on a VLAN using the following syntax and commands:

`config vlan <vid> ipx` followed by:	
`info`	Displays the switch IPX configuration.
`create <IPX-network-number> [<encapsulation>]`	Creates a protocol-based VLAN using one of the supported encapsulation methods as the protocol: • network number is the destination IPX network number for the route. • vid is the VLAN ID in a range from 1 to 4095. • <encapsulation> is <ipx802dot3 | ipx802dot2 | ipxSnap | pxEthernet2>.
`delete <IPX-network-number>`	Deletes the specified IPX network.

config ipx set commands

The **config ipx set** commands configure maximum entries for IPX parameters and use the following options:

config ipx set followed by:	
info	Displays current maximum entries set on the switch (Figure 175).
max-route <*max_entries*>	Sets the maximum number of IPX routes that can be learned by the switch. **Note**: To take effect, the configuration must be saved and the switch reset.
max-sap <*max_entries*>	Sets the maximum number of IPX services that can be learned by the switch. **Note**: To take effect, the configuration must be saved and the switch reset.
max-static-route <*max_entries*>	Sets the maximum number of static IPX routes that can be configured on the switch. **Note**: To take effect, the configuration must be saved and the switch reset.
max-static-sap <*max_entries*>	Sets the maximum number of static IPX services that can be configured on the switch. **Note**: To take effect, the configuration must be saved and the switch reset.

Figure 175 config ipx set info command output

```
Passport 1200# config ipx set info
                      max-route - 128
                        max-sap - 1500
                max-static-route - 128
                  max-static-sap - 64
                         netbios - ON
```

config ipx static-route commands

The **ipx static-route** commands are used to create or delete a static IPX network route. The commands use the following options:

config ipx static-route followed by:	
info	Displays IPX routes created and/or deleted (Figure 176).
create <*IPX-network-number*> <*nexthop*> <*hop-count*> <*tick-count*>	Creates a static IPX network route where: • *nexthop* is the IPX address of the next router. • *hop-count* is the number of passes through a router. • *tick-count* is the number of ticks (1/18th of a second). To create a default route, enter FF:FF:FF:FE as the IPX network number.
delete <*IPX-network-number*>	Deletes the static IPX network route.

Figure 176 config ipx static-route info command output

```
Passport 1200# config ipx static-route info

Sub-Context: clear config monitor show test trace
Current Context:

               create :
               delete : N/A
```

config ipx rip commands

The **config ipx rip** commands are used to configure Routing Information Protocol (RIP) on IPX interfaces. The following three timing parameters control IPX RIP behavior:

- Hold-multiplier
- Delay-timer
- Interval-timer

If the global default parameters are going to be different from the factory default, set the default parameters prior to setting individual interface parameters.

config ipx rip default command

The **config ipx rip default** commands set the IPX RIP default values using the following options:

config ipx rip default followed by:	
-delay <*delay-timer*>	Sets the delay timer default values in milliseconds. The range is 1 to 1000; the default is 50 ms.
-hold-multiplier <*age-multiplier*>	Sets the hold multiplier default value. The range is 1 to 2147483647; the default is 3.
-interval <*interval-timer*>	Sets the interval timer default values in seconds. The range is 1 to 2147483647; the default is 60 seconds.

config ipx rip info command

The **config ipx rip info** command displays IPX RIP settings on the switch.

Figure 177 shows output for the **config ipx rip info** command.

Figure 177 config ipx rip info command output

```
Passport 1200# config ipx rip info

Sub-Context: clear config monitor show test trace
Current Context:

                  default-delay : 50 msec
        default-hold-multiplier : 3
               default-interval : 60 sec

      hold-multiplier :
                state :
         update-delay :
      update-interval :
```

config ipx rip command

The **config ipx rip** commands set the IPX RIP interface values using the following options:

config ipx rip followed by:	
age-multiplier <*IPX-network-number*> <*age-multiplier*>	Sets the hold multiplier value for the IPX interface. The range is 1 to 2147483647; the default is 3.
state <*IPX-network-number*> <*on|off*>	Enables or disables RIP for the given IPX network number.
update-delay <*IPX-network-number*> <*delay-timer*>	Sets the update delay timer for the IPX interface. The range is 1 to 1000 ms; the default is 50 ms.
update-interval <*IPX-network-number*> <*interval-timer*>	Sets the update interval for the IPX interface in seconds. The range is 1 to 2147483647. The default is 60 seconds.

config ipx sap commands

The **IPX SAP** commands are used to configure Service Advertisement Protocol (SAP) on IPX interfaces. Three timing parameters also control IPX SAP behavior:

- Hold-multiplier
- Delay-timer
- Interval-timer

If the global default parameters are going to be different from the factory defaults, set the default parameters prior to setting individual interface parameters.

config ipx sap info command

The **config ipx sap info** command displays IPX SAP settings.

Figure 178 shows output for the **config ipx sap info** command.

Figure 178 config ipx sap info command output

```
Passport 1200# config ipx sap info

Sub-Context: clear config monitor show test trace
Current Context:

              create :
              delete : N/A

                 default-delay : 50 msec
       default-hold-multiplier : 3
              default-interval : 60 sec

     hold-multiplier :
        update-delay :
     update-interval :
```

config ipx sap default

The **config ipx sap default** command sets the global default values using the following options:

config ipx sap default followed by:	
-delay <*delay-timer*>	Sets the delay timer default values in milliseconds. The range is 1 to 1000; the default is 50 ms.
-hold-multiplier <*age-multiplier*>	Sets the hold multiplier default value. The range is 1 to 2147483647; the default is 3.
default-interval <*interval-timer*>	Sets the interval timer default values in seconds. The range is 1 to 2147483647; the default is 60 seconds.

config ipx sap command

The **config ipx sap** command sets the IPX SAP parameters using the following options:

config ipx sap followed by:	
create <*service-type*> <*service-name*> <*ipxhost*> <*socket-number*> <*hop-count*>	Creates a static SAP entry where: • Service type is defined by an integer (1-65535). Examples include: 0000h = unknown 0003h = print queue 0004h = file server 0005h = job server 0007h = print server 0009h = archive server 0024h = remote bridge server 0047h = advertising print server • *service name* is a character string (1 to 47 characters). • *ipxhost* is the network and node (network = IPX network number. 1-2147483647;node = xx:yy:zz:uu:vv:ww, where xx, yy, zz, uu, yy, and ww are 2-digit hexadecimal numbers). • *socket-number* is 0-65535. • *hop-count* is 1 to 15.
delete <*service-name*>	Deletes a static SAP entry.
age-multiplier <*IPX-network-number*> <*age-multiplier*>	Sets the hold multiplier value for the IPX interface. The range is 1 to 2147483647; the default is 3.
update-delay <*IPX-network-number*> <*delay-timer*>	Sets the update delay timer for the IPX interface. The range is 1 to 1000 ms; the default is 50 ms.
update-interval <*IPX-network-number*> <*interval-timer*>	Sets the update interval for the IPX interface in seconds. The range is 1 to 2147483647; the default is 60 seconds.

show ipx commands

The show ipx commands display the configuration of IPX on the switch.

show ipx config command

The **show ipx config** command displays general IPX configuration information for the switch or for a specified IPX network number.

The command syntax is:

show ipx config [<IPX-network-number>]

show ipx default command

The **show ipx default** command displays the current IPX RIP and SAP timer default values.

Figure 179 shows output for the **show ipx default** command.

Figure 179 show ipx default command output

```
Passport 1200# show ipx default

================================================================================
                                    Ipx Default Values
================================================================================
RIP Hold-Multiplier: 3
RIP Delay-Timer:     50 msec (20 per sec)
RIP Update-Timer:    60 sec
SAP Hold-Multiplier: 3
SAP Delay-Timer:     50 msec (20 per sec)
SAP Update-Timer:    60 sec
```

show ipx route command

The **show ipx route** command displays information about the IPX routes on the switch or a specific IPX route, including the following information:

- Type
- Hop count
- Ticks

The command syntax is:

show ipx route [<*IPX-network-number*>] [<*IPX-network-number*>]

show ipx sap command

The **show ipx sap** command displays information about IPX SAP on the switch for all SAP services or a specified service.

The command syntax is:

```
show ipx sap [<service-name>]
```

show ipx stats command

The **show ipx stats** command displays IPX statistics for the specified IPX network number.

The command syntax is:

```
show ipx stats <IPX-network-number>
```

Figure 180 shows output for the **show ipx stats** command.

Figure 180 show ipx stats command output

```
Passport 1200# show ipx stats
CIRCUIT_ID      NETNUM      RIP_TX      RIP_RX      SAP_TX      SAP_RX

-----------------------------Total---------------------------------
                               0           0           0           0

Bad checksum          0
Received packet       0
Too many hops         0
Header error          0
Unknown socket        0
Input discard         0
Forward packet        0
Output request        0
Output no route       0
Malformed request     0
Output discard        0
Output packet         0
Resource failure      0
Bad rip               0
Bad sap               0
```

show vlan info ipx command

The **show vlan info ipx** command displays VLAN IPX information for a specified VLAN or for all VLANs.

The command syntax is:

```
show vlan info ipx [<vid>]
```

Chapter 7
Configuring IP flow, policies, and filters

Caution: IP Multicast with IGMP and DVMRP is not supported on this platform.

This chapter describes the CLI commands used to configure IP flows, policies, and filters. The following major sections are included:

- "IP flow commands," next
- "IP policies" on page 279
- "IP filters" on page 294

IP flow commands

The **`config IP flow`** commands are used to set priority. You can use IP flows to identify a particular stream of traffic at the IP layer and at the TCP/UDP layer.

config ip flow commands

The **config ip flow** commands include the following options:

config ip ipflow followed by:	
info	Displays the current IP flow settings (Figure 181).
create src-ip <*value*> src-port <*value*> dst-ip <*value*> dst-port <*value*> protocol <*value*>	Creates an IP flow with the following parameters: • src-ip <value> is the source IP address of an IP packet {a.b.c.d}. • src-port <value> is the source port of an IP packet. The source IP port range is 0 to 65535. A zero value in this field can be used as a wildcard value. • dst-ip <value> is the destination IP address of an IP packet {a.b.c.d}. • dst-port <value> is the destination port of an IP packet. A zero in this field is used as a wildcard (0 to 65535). • protocol <value> is the protocol type: IP, TCP, or UDP.
delete src-ip <*value*> src-port <*value*> dst-ip <*value*> dst-port <*value*> protocol <*value*>	Deletes an IP flow. The parameters are the same as described for create.

Figure 181shows output for the **config ip flow** command.

Figure 181 config ip flow command output

```
swlab-edge2# config ip ipflow info

Sub-Context: clear config monitor show test trace
Current Context:

                    create : not created
                    delete : N/A
```

show ip flow command

The **show ip flow** command displays the source and destination IP address, the source and destination IP port address, and the protocol for IP flow configuration.

Figure 182 shows output for the **show ip flow** command.

Figure 182 show ip flow command output

```
Passport 1100# show ip flow

================================================================================
                                    Ip Flow
================================================================================
SRC_IPADDR          SRC_IPPORT DST_IPADDR          DST_IPPORT PROTOCOL
--------------------------------------------------------------------------------
Passport 1100#
```

IP policies

The **ip policy** commands allow you to configure and view IP policy features supported on a Passport 1000 Series switch. The accept and announce policies can be configured for the switch according to the selected protocol (RIP or OSPF). A policy is made up of three parts:

- Matching criteria
- Set parameters
- Action

The matching criteria are used to decide whether a policy should be applied to a certain route.

After an announce policy is selected for a route, the set parameters are used to construct the route advertisement. After an accept policy is selected for a route, the set parameters are used to introduce the route into the routing table.

config ip policy commands

Several categories of IP policy commands are available:

- "config ip policy info command" on page 280
- "config ip policy addrlist command" on page 280
- "config ip policy netlist command" on page 281

- "config ip policy ospf command" on page 282
- "config ip policy rip commands" on page 285

config ip policy info command

The **config ip policy info** command displays the current policy settings on the switch.

config ip policy addrlist command

The **config ip policy addrlist** command sets address list matching criteria to suit a given route. The parameter `listid` is the address list ID (1 to 1000). The commands include the following options:

config ip policy addrlist <listid> followed by:	
`info`	Displays the address list characteristics (Figure 183).
`add-address <ipaddr>`	Adds an IP address to the policy address list.
`create`	Creates a policy address list.
`delete`	Deletes a policy address list.
`name <name>`	Assigns a name to the policy address list.
`remove-address <ipaddr>`	Removes an address from the policy address list.

Figure 183 shows output for the **config ip policy addrlist info** command.

Figure 183 config ip policy addrlist info command output

```
Passport 1100# config ip policy addrlist 3 info

Sub-Context: clear config monitor show test trace
Current Context:

                      create : not created
                      delete : not created
                        name : not created
                 add-address : not created
              remove-address : not created
```

config ip policy netlist command

The **config ip policy netlist** commands set network list matching criteria to suit a given route where listid is the network list ID (1 to 1000). The commands include the following options:

config ip policy netlist <listid> followed by:	
info	Displays settings for the IP policy network list (Figure 184).
add-network <*ipaddr/mask*>	Adds a network with the IP address and subnet mask to the policy network list.
create	Creates a policy network list.
delete	Deletes the policy network list.
name <*name*>	Assigns a name to the policy network list.
remove-network <*ipaddr/mask*>	Removes an address from the policy address list.

Figure 184 shows output for the **config ip policy netlist info** command.

Figure 184 config ip policy netlist info command output

```
Passport 1100# config ip policy netlist info
object <listid> = info is out of range
object <listid> required
<listid>         = list id {1..1000}

policy netlist commands
add-network      add network to network list
create           create a network list
delete           delete a network list
info             show current level parameter settings and next level directories
name             set network list name
remove-network _remove network from network list
```

config ip policy ospf command

The **config ip policy ospf** commands are used to globally apply the configured OSPF accept or announce policies. After you set up OSPF policies, you must apply the policies before they take effect. The commands include the following options:

config ip policy ospf followed by:	
info	Displays global status of OSPF accept and announce policies.
ospf apply-accept	Globally applies OSPF accept policies.
ospf apply-announce	Globally applies OSPF announce policies.

Note: Although individual policies can be configured and enabled, they will not take effect until the global apply command is issued.

config ip policy ospf accept command

The **config ip policy ospf accept** commands allow you to configure the OSPF accept policy with a policy ID range from 6001 to 7000. The commands include the following options:

config ip policy ospf accept <pid> followed by:	
info	Displays the current OSPF accept policy settings (Figure 185).
action <*accept*|*ignore*>	Selects whether the OSPF policy action will be to accept or ignore external route information.
create	Creates an OSPF accept policy.
delete	Deletes an OSPF accept policy.
disable	Disables an OSPF accept policy.
enable	Enables an OSPF accept policy.

config ip policy ospf accept <pid> followed by:	
exact-net-list <*netlist id*>	Sets an OSPF accept policy in which networks only match the specific network advertisement. The netlist id range is 0 to 1000.
ext-metric-type <*type1*|*type2*>	Sets the OSPF accept policy external metric type to type 1 or type 2.
name <*name*>	Assigns the OSPF accept policy name.
precedence <*precedence*>	Sets the precedence for the OSPF accept policy. The range is 0 to 65535. If multiple policies apply, the higher precedence is used.
range-net-list <*netlist id*>	Sets the OSPF accept policy to match any network number that falls into the indicated range. The netlist id range is 0 to 1000.

Figure 185 shows output for the **config ip policy ospf accept info** command.

Figure 185 config ip policy ospf accept info command output

```
Passport 1100# config ip policy ospf accept info
object <pid> = info is out of range
object <pid> required
<pid>             = policy id {6001..7000}

ospf accept commands
action           set accept or ignore
create           create ospf accept policy
delete           delete ospf accept policy
disable          disable ospf accept policy
enable           enable ospf accept policy
exact-net-list   set ospf accept policy exact net list
ext-metric-type set ospf accept policy ext metric type
info             show current level parameter settings and next level directories
inject-net-list set ospf accept policy inject net list
name             set ospf accept policy name
precedence       set ospf accept policy precedence
range-net-list   set ospf accept policy range net list
```

config ip policy ospf announce command

The **config ip policy ospf announce** commands allow you to configure the OSPF announce policy, where the OSPF announce policy ID is in the range 2001 to 3000. The commands use the following options:

config ip policy ospf announce <pid> followed by:	
info	Displays the settings for the OSPF announce policy (Figure 186).
action <*accept*|*ignore*>	Selects whether the OSPF policy action accepts or ignores external route information.
add-route-source <*direct*|*static*|*rip*|*any*>	Adds a route source to the announce policy; sets direct, static, RIP, or any as accepted sources from which the route can be learned.
advertise-netlist <*netlist id*>	If the action is set to announce, allows sending or advertising networks that differ from the actual network in the routing table. The netlist ID is the advertised netlist ID (0 to 1000) and allows advertisement of an aggregate or default along with the actual network.
create	Creates an OSPF announce policy.
delete	Deletes an OSPF announce policy.
disable	Disables an OSPF announce policy.
enable	Enables an OSPF announce policy.
exact-net-list <*netlist id*>	Sets an OSPF announce policy in which networks only match the specific network advertisement. The netlist id range is 0 to 1000.
ext-metric <*ext-metric*>	Sets the OSPF announce external metric (0 to 65535).
ext-metric-type <*type1*|*type2*>	Sets the OSPF announce policy external metric type to type 1 or type 2.
name <*name*>	Assigns the OSPF accept policy name.
precedence <*precedence*>	Sets the precedence for the OSPF announce policy. The range is 0 to 65535. If multiple policies apply, the higher precedence is used.
range-net-list <*netlist id*>	Sets the OSPF announce policy to match any network number that falls into the indicated range. The netlist id range is 0 to 1000.

config ip policy ospf announce <pid> followed by:	
remove-route-source <*direct*|*static*|*rip*|*any*>	Removes a route source from the announce policy.
rip-gateway-list <*addrlist id*>	Identifies the RIP gateway lists that are associated with this announce policy. The RIP gateway list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.
rip-interface-list <*addrlist id*>	Indicates the entries in the RIP interface lists that are associated with this announce policy. The RIP interface list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.

Figure 186 shows output for the **config ip policy ospf announce info** command.

Figure 186 config ip policy ospf announce info command output

```
Passport 1100# config ip policy ospf announce 2002 info

Sub-Context: clear config monitor show test trace
Current Context:

                      action : not created
           add-route-source : not created
         advertise-net-list : not created
                     create : not created
                     delete : not created
                     enable : not created
          exact-net-list : not created
            exact-metric : not created
         ext-metric-type : not created
                    name : not created
              precedence : not created
           range-netlist : not created
       remove-route-source : not created
          rip-gateway-list : not created
       rip-interface-list : not created
```

config ip policy rip commands

The **config ip policy rip** commands are used to apply the configured RIP accept or announce policies to the switch. Use the **config ip policy rip info** command to display current status.

config ip policy rip accept commands

The **config ip policy rip accept** commands allow you to configure the RIP accept policy, where pid is the RIP accept policy ID (4001 to 5000). The commands use the following options:

config ip policy rip accept <pid> followed by:	
info	Displays the settings for the RIP accept policy (Figure 187).
action <*accept*|*ignore*>	Selects whether the RIP policy action accepts or ignores matches.
apply-mask <*ipmask*>	Sets an IP subnet mask for the RIP accept policy, where <ipmask> is the apply-mask {a.b.c.d}.
create	Creates a RIP accept policy.
delete	Deletes a RIP accept policy.
disable	Disables a RIP accept policy.
enable	Enables a RIP accept policy.
inject-net-list <*netlist id*>	Sets a RIP accept policy that inserts networks into the routing table that differ from the actual advertised network. The inject-net-list ID range is 0 to 1000.
name <*string*>	Assigns a RIP accept policy name.
precedence <*precedence*>	Sets the precedence for the OSPF accept policy. The range is 0 to 65535. If multiple policies apply, the higher precedence is used.
range-net-list <*netlist id*>	Sets the RIP accept policy to match any network number that falls into the indicated range. The netlist id range is 0 to 1000.
rip-gateway-list <*addrlist id*>	Identifies the RIP gateway lists that are associated with this policy. The RIP gateway list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.
rip-interface-list <*listid*>	Indicates the entries in the RIP interface lists that are associated with this policy. The RIP interface list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.

Figure 187shows output for the **config ip policy rip accept info** command.

Figure 187 config ip policy rip accept info command output

```
Passport 1200# config ip policy rip accept info
object <pid> = info is out of range
object <pid> required
<pid>            = policy id {4001..5000}

rip accept commands
action          set accept or ignore
apply-mask      set apply mask
create          create rip accept
delete          delete rip accept
disable         disable rip accept
enable          enable rip accept
exact-netlist   set exact net list
info            show current level parameter settings and next level directories
inject-netlist  set inject netlist
name            set rip accept list name
precedence      set rip accept policy precedence
range-netlist   set range netlist
rip-gateway-listset rip gateway list
rip-interface-listset rip interface list
```

config ip policy rip announce command

The **config ip policy rip announce** commands allow you to configure the RIP announce policy, where pid is the RIP announce policy ID (1 to 1000). The commands use the following options:

config ip policy rip announce <pid> followed by:	
info	Displays the settings for the RIP announce policy (Figure 188).
action <*accept*|*ignore*>	Selects whether the RIP policy action accepts or ignores matches.
add-route-source <*direct*|*static*|*rip*|*ospf*|*any*>	Adds a route source to the announce policy.
advertise-netlist <*netlist id*>	If the action is set to announce, allows sending or advertising networks that differ from the actual network in the routing table advertise network list ID (0 to 1000).
create	Creates a RIP announce policy.
delete	Deletes a RIP announce policy.
disable	Disables a RIP announce policy.

config ip policy rip announce <pid> followed by:	
enable	Enables a RIP announce policy.
exact-net-list <*netlist id*>	Sets a RIP announce policy exact network list, where the exact-network list ID is 0 to 1000.
name <*string*>	Assigns a RIP accept policy name.
ospf-router-id-list <*addrlist id*>	Indicates the entries in the OSPF router lists that are associated with this policy. ospf-rtr-list <listid> is the OSPF router-ID list ID (0 to 1000). It is valid only for OSPF-routed sourced routes if OSPF is included as a route source.
ospf-route-type <*type1*|*type2*|*external*|*internal*|any>	Indicates the entries in the OSPF router lists that are associated with this policy: type 1, type 2, external routes, internal routes, or any OSPF routes.
outbound-interface-list <*addrlist id*>	Indicates the entries in the outbound lists that are associated with this policy.
precedence <*precedence*>	Sets the precedence for the OSPF accept policy. The range is 0 to 65535. If multiple policies apply, the higher precedence is used.
range-net-list <*netlist id*>	Sets the RIP announce policy range network list. The range is 0 to 1000.
remove-route-src <*direct*|*static*|*rip*|*ospf*|*any*>	Removes a route source from the announce policy.
rip-gateway-list <*addrlist id*>	Identifies the RIP gateway lists that are associated with this policy. The RIP gateway list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.
rip-interface-list <*listid*>	Indicates the entries in the RIP interface lists that are associated with this policy. The RIP interface list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.
rip-metric <*rip-metric*>	Sets the RIP external metric (0 to 15) for the policy, the external metric to use when advertising a route that matches this policy. Meaningful only if the set action is announce.

Figure 188 shows output for the **config ip policy rip announce info** command.

Figure 188 config ip policy rip announce info command output

```
Passport 1100# config ip policy rip announce 3 info

Sub-Context: clear config monitor show test trace
Current Context:

                      action : not created
          add-route-source : not created
        advertise-net-list : not created
                      create : not created
                      delete : not created
                      enable : not created
           exact-net-list : not created
                        name : not created
          ospf-router-list : not created
           ospf-route-type : not created
      outbound-interface-list : not created
              precedence : not created
           range-netlist : not created
       remove-route-source : not created
          rip-gateway-list : not created
        rip-interface-list : not created
              rip-metric : not created
```

show ip policy commands

The **`show ip policy`** commands provide information about the IP policies that are set up on the switch.

show ip policy addrlist info command

The **`show ip policy addrlist info`** command displays the IP policy address lists set on the switch. If an address list ID is not entered, all address lists on the switch are listed.

The command syntax is:

`show ip policy addrlist info [id <`*`value`*`>]`

Figure 189 shows output for the **`show ip policy addrlist info`** command.

Figure 189 show ip policy addrlist info command output

```
Passport 1100# show ip policy addrlist info

================================================================================
                                    Policy AddrList
================================================================================
ID   NAME
--------------------------------------------------------------------------------
1    kh
```

If an address list ID is entered, the display lists the addresses belonging to that list

Figure 190 shows output for the **`show ip policy addrlist info id 1`** command.

Figure 190 show ip policy addrlist info id 1 command output

```
Passport 1100# show ip policy addrlist info id 1

================================================================================
                                    Policy AddrList
================================================================================
ID   NAME
--------------------------------------------------------------------------------
1    kh

IpAddr
---------------
1.1.1.1
2.2.2.2
```

show ip policy netlist info command

The **`show ip policy netlist info`** command displays the network lists on the switch.

The command syntax is:

`show ip policy netlist info [id <value>]`

If no ID is entered, information is displayed about all network lists on the switch.

Figure 191 shows output for the **`show ip policy netlist info`** command.

Figure 191 show ip policy netlist info command output

```
Passport 1100# show ip policy netlist info

================================================================================
                                    Policy NetList
================================================================================
ID   NAME
--------------------------------------------------------------------------------
1    vdf4
```

If an ID is entered, information is displayed about that network list only.

Figure 192 shows output for the **show ip policy netlist info** command.

Figure 192 show ip policy netlist info id 1 command output

```
Passport 1100# show ip policy netlist info id 1

================================================================================
                                    Policy NetList
================================================================================

ListId: 1    Name: vdf4
NetAddr         NetMask
--------------- ---------------
12.1.1.0        255.255.255.0
```

show ip policy ospf accept info command

The **show ip policy ospf accept info** command displays information about the OSFP accept policies configured on the switch. If an ID is not entered, the display provides information for all OSPF accept policies on the switch. If a policy ID is entered, the display lists information for only that policy.

The command syntax is:

```
show ip policy ospf accept info [id <value>]
```

show ip policy ospf accept lists command

The **show ip policy ospf accept lists** command displays the accept lists on the switch. If an ID is not entered, all OSPF accept lists are displayed. If an ID is entered, only that list is displayed.

The command syntax is:

```
show ip policy ospf accept lists [id <value>]
```

show ip policy ospf accept match network command

The **`show ip policy ospf accept match network`** command lists the policies that match the specified network with a range or exact match.

The command syntax is:

```
show ip policy ospf accept match network <value>
```

show ip policy ospf announce info command

The **`show ip policy ospf announce info`** command displays information about the OSFP announce policies configured on the switch. If an ID is not entered, the display provides information for all OSPF announce policies on the switch. If a policy ID is entered, the display lists information for only that policy.

The command syntax is:

```
show ip policy ospf announce info [id <value>]
```

show ip policy ospf announce lists command

The `show` **`ip policy ospf announce lists`** command displays list characteristics of the OSPF announce policies configured on the switch or for a specified policy ID.

The command syntax is:

```
show ip policy ospf announce lists [id <value>]
```

show ip policy ospf announce match network command

The **`show ip policy ospf announce match`** command lists the policies that match the specified network with a range or exact match.

The command syntax is:

```
show ip policy ospf announce match network <value>
```

show ip policy rip accept info command

The **show ip policy rip accept info** command displays information about the RIP accept policies configured on the switch. If an ID is not entered, the display provides information for all RIP accept policies on the switch. If a policy ID is entered, the display lists information for only that policy.

The command syntax is:

```
show ip policy rip accept info [id <value>]
```

show ip policy rip accept lists command

The **show ip policy rip accept lists** command displays the accept lists on the switch in the syntax. If an ID is not entered, all OSPF accept lists are displayed. If an ID is entered, only that list is displayed.

The command syntax is:

```
show ip policy ospf accept lists [id <value>]
```

show ip policy rip accept match network command

The **show ip policy rip accept match network** command lists the policies that match the specified network with a range or exact match.

The command syntax is:

```
show ip policy rip accept match network <value>
```

show ip policy rip announce info command

The **show ip policy rip announce info** command displays information about RIP announce policies on the switch or about a specified RIP announce policy.

The command syntax is:

```
show ip policy rip announce info [id <value>]
```

show ip policy rip announce lists command

The **`show ip policy rip-announce lists`** command displays information about RIP announce policy lists on the switch, or about a specific RIP announce policy list.

The command syntax is:

```
show ip policy rip-announce lists [id <value>]
```

show ip policy rip announce match network command

The **`show ip policy rip announce match network`** command lists the policies that match the specified network with a range or exact match. The command syntax is:

```
show ip policy rip announce match network <value>
```

IP filters

IP filters on Passport routing switches can be used to manage traffic and, in some cases, provide security. Each filter set includes match conditions and actions to be performed when a match condition is satisfied.

Note: Implementation of IP traffic filters requires -A (ARU2) or later hardware.

Packet filters apply to all routed packets to be forwarded through the routing switch on specified ingress ports. The filter sets are applied to the port and a default action (forward or drop) is set for the port. All packets not matching any filter take the default action. Packets matching a single filter with the opposite action will take that action. For more information about filtering, refer to *Networking Concepts for the Passport 1000 Series Switch*.

config ip filter commands

The following command topics are included in this section:

- "config ip traffic-filter commands" on page 295
- "config ip traffic-filter create commands" on page 296
- "config ip traffic-filter filter commands" on page 296
- "config ip traffic-filter filter action command" on page 297
- "config ip traffic-filter filter match commands" on page 299
- "config ip traffic-filter global-set commands" on page 300
- "config ip traffic-filter set commands" on page 300
- "config ethernet ip traffic-filter commands" on page 301

config ip traffic-filter commands

The generic filter commands use the following options:

config ip traffic-filter followed by:	
info	Displays IP traffic filter settings (Figure 193).
clear-stats [<*fid*>]	Clears filter statistics for the specified filter ID where the traffic filter ID range is 1 to 4000.
log-interval <*seconds*>	Sets the filter log interval for traffic filter statistics logging in seconds (0 to 36000).

Figure 193 shows output for the **config ip traffic-filter info** command.

Figure 193 config ip traffic-filter info command output

```
swlab-edge2# config ip traffic-filter info

Sub-Context: clear config monitor show test trace
Current Context:

                log-interval : 5
                 clear-stats : N/A
```

config ip traffic-filter create commands

The **config ip traffic-filter create** commands are used to configure source, destination, and global traffic filters for the interface. These commands use the following options:

config ip traffic-filter create followed by:	
info	Displays the destination, source, and global filters that have been created.
destination dst-ip <*value*> [src-ip <*value*>] [id <*value*>]	Creates a destination filter: • dst-ip <value> is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • src-ip <value> is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.
global [src-ip <*value*>] [dst-ip <*value*>] [id <*value*>]	Creates a global filter: • src-ip <value> is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x |default}. • dst-ip <value> is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.
source src-ip <*value*> [dst-ip <*value*>] [id <*value*>]	Creates a source filter: • src-ip <value> is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • dst-ip <value> is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.

config ip traffic-filter filter commands

The **config ip traffic-filter** commands are the general **config ip traffic-filter filter** commands, where <fid> is the traffic filter ID (1 to 4000).

The commands use the following options:

config ip traffic-filter filter <fid> followed by:	
info	Displays the settings for the specified filter.
delete	Deletes the specified traffic filter.

config ip traffic-filter filter <fid> followed by:	
log-stats <*enable*|*disable*>	Enables or disables the logging of statistics for the filter.
name <*name*>	Gives a name to the filter where name <value> is the IP filter name {string}.
modify info	Displays modifications to filter VLAN tagging or DiffServ settings.
modify diffserv-rule <*none*|*rule1*|*rule2*|*rule3*>	Modifies the differentiated service rule used by the switch. Refer to page 182 for information about Differentiated Services.
modify vlan-tag-priority <*vlan-priority-number*>	Sets the IEEE VLAN priority for the filter using a number in the range of 1 to 7.

Figure 194 shows output for the **config ip traffic-filter filter info** command.

Figure 194 config ip traffic-filter filter info command output

```
swlab-edge2# config ip traffic-filter filter 1 info

Sub-Context: clear config monitor show test trace
Current Context:

                    delete : N/A
                log-stats : not created
                     name : not created
```

config ip traffic-filter filter action command

The **config ip traffic-filter filter action** commands are used to set action parameters for IP filters by enabling or disabling the filters where <fid> is the traffic filter ID (1 to 4000). The commands use the following options:

config ip traffic-filter filter <fid> action followed by:	
info	Displays configure actions for the filter (Figure 195).
mode <*default*|*forward*|*drop*>	Sets the action to occur when a filter is applied (the default action, forward the packet, or drop the packet).

config ip traffic-filter filter <fid> action followed by:	
mirror <*enable*|*disable*>	Enables or disables the traffic filter mirror option.
high-priority <*enable*|*disable*>	Enables or disables the traffic filter high-priority option.
tcp-connect <*enable*|*disable*>	Enables or disables the traffic filter TCP-connect option, which allows only TCP connections established from within the network (enabled) or allows bidirectional establishment (disabled).
use-packet-limit <*enable*|*disable*>	Enables or disables the traffic filter use packet limit option.

Figure 195 shows output for the **config ip traffic-filter filter action info** command.

Figure 195 config ip traffic-filter filter action info command output

```
swlab-edge2# config ip traffic-filter filter 1 action info

Sub-Context: clear config monitor show test trace
Current Context:

                        mode : not created
                      mirror : not created
               high-priority : not created
                 tcp-connect : not created
                dffserv-rule : not created
               use-pkt-limit : not created
```

config ip traffic-filter filter match commands

These commands are the traffic filter match commands where `<fid>` is the traffic filter ID (1 to 4000). The commands use the following options:

config ip traffic-filter filter <fid> match followed by:	
`info`	Displays the matching settings for the filter.
`dst-port <port> [dst-option <value>]`	Sets the TCP/UDP destination port and destination option. • <port> is the TCP/UDP destination port to filter on (0 to 65535). • dst-option <value> is the TCP/UDP destination port option. {ignore|equal|less|greater|notequal}.
`packet-limit <pktlimit>`	Sets the packet limit (number of hits) for the filter. When the limit is reached, the filter stops applying action. The range is 0 to 65535.
`protocol <protocoltype>`	Sets the protocol type for the filter, where protocol type is: • ignore • ICMP • TCP • UDP
`src-port <port> [src-option <value>]`	Sets the TCP/UDP source port and source option. • <port> is the TCP/UDP source port to filter on (0 to 65535). • src-option <value> is the option {ignore|equal|less|greater|notequal}.

config ip traffic-filter global-set commands

The **config ip traffic-filter global-set** commands configure the IP traffic filter global list where <setid> is the global set ID (1 to 100). The commands use the following options:

config ip traffic-filter global-set <setid> followed by:	
info	Displays the global set characteristics.
add-filter <*fid*>	Adds a global filter to a global set with the traffic filter ID range of 1 to 4000.
create [name <*value*>]	Creates a global set where name <value> is the set name {string}.
delete	Deletes a global set.
remove-filter <*fid*>	Removes a global filter from a global set.

config ip traffic-filter set commands

The **config ip traffic-filter set** commands configure the filter set where <setid> is the set ID (300 to 1000). The commands use the following options:

config ip traffic-filter list <setid> followed by:	
info	Displays the filter set characteristics.
add-filter <*fid*>	Adds a filter to a filter set where the traffic filter ID has a range of 1 to 4000.
create [name <*value*>]	Creates a filter set with the name {string}.
delete	Deletes a filter set.
remove-filter <*fid*>	Removes a filter from a filter set.

config ethernet ip traffic-filter commands

The **config ethernet ip traffic-filter** commands are used at the port level to set filters used to manage traffic. Each filter set includes match conditions and actions to be performed when a match condition is satisfied. These commands include <ports> as the portlist {slot/port[-slot/port][,...]}.

config ethernet <ports> ip traffic-filter followed by:	
info	Displays the traffic filters applied to the port.
default-action forward	Sets the port filter default action to forward.
default-action drop	Sets the port filter default action to drop.
default-action info	Displays the port default action configuration.
add set <*value*>	Adds a filter to a port, where set <value> is the filter set ID (1 to 1000).
create	Creates a traffic filtering entity on a port.
delete	Removes filtering from a port.
disable	Disables filtering on a port.
enable	Enables filtering on a port.
remove set <*value*>	Removes a filter set from a port where set <value> is the filter set ID (1 to 1000).

show ip traffic-filter commands

The following commands provide information about the IP traffic filters.

show ip traffic-filter active command

The **show ip traffic-filter active** command displays a list of active filters or returns the information that there are no active filters.

show ip traffic-filter destination command

The **show ip traffic-filter destination** command displays the source and destinations for the active traffic filters. If a filter ID (fid) is entered, data is displayed for the specific filter. Otherwise, all filters are shown.

The command syntax is:

```
show ip traffic-filter destination [<fid>]
```

show ip traffic-filter disabled command

The command displays information about the disabled filters on the switch. If port numbers are entered, information is displayed only for those ports.

The command syntax is:

```
show ip traffic-filter disabled [<ports>]
```

show ip traffic-filter enabled command

The **show ip traffic-filter enabled** command displays information about the enabled filters on the switch or on specified ports.

The command syntax is:

```
show ip traffic-filter enabled [<ports>]
```

show ip traffic-filter global command

The **show ip traffic-filter global** command displays global filters for a switch or for specified filter IDs.

The command syntax is:

```
show ip traffic-filter global [<fid>]
```

show ip traffic-filter info global-set command

The **show ip traffic-filter info global-set** command displays information about a specified global filter list or all global filter lists on the switch.

The command syntax is:

```
show ip traffic-filter info global-set [<id>]
```

show ip traffic-filter info list command

The **show ip traffic-filter info list** command displays traffic-filter information for a specified list or for all lists.

The command syntax is:

```
show ip traffic-filter info list [<id>]
```

show ip traffic-filter interface command

The **show ip traffic-filter interface** command displays information about the traffic filter interface for a switch or for specified ports.

The command syntax is:

```
show ip traffic-filter interface <ports>
```

show ip traffic-filter log-interval command

The **show ip traffic-filter log-interval** command displays the logging interval for the traffic filter.

show ip traffic-filter source command

The **show ip traffic-filter source** command displays information about the filter source for a specified filter or for all filters.

The command syntax is:

```
show ip traffic-filter source [<fid>]
```

show ip traffic-filter stats command

The **`show ip traffic-filter stats`** command displays the filter ID and counter information for all filters or a specified filter ID.

The command syntax is:

```
show ip traffic-filter stats [<fid>]
```

Chapter 8
Monitor commands

Caution: IP Multicast with IGMP and DVMRP is not supported on this platform.

The monitor commands are self-updating **`show`** commands. Set the monitor duration and interval using the following commands:

- **`config cli monitor duration <integer>`**
  where duration is in seconds, 1 to 1800
- **`config cli monitor interval <integer>`**
  where interval is in seconds, 1 to 600

To clear the display, press Ctrl/L.

Table 13 lists the available monitor commands and a page reference for the corresponding **`show`** command.

Table 13 Monitor and show commands

Monitor commands	Corresponding show command page reference
monitor mlt error collision [<mid>]	page 147
monitor mlt error main [<mid>]	page 148
monitor mlt stats interface main [<mid>]	page 149
monitor mlt stats interface utilization [<mid>]	page 306
monitor ports error collision [<ports>]	page 130
monitor ports error extended [<ports>]	page 132
monitor ports error main [<ports>]	page 148
monitor ports error ospf [<ports>]	page 234
monitor ports stats bridging [<ports>]	page 135

Table 13 Monitor and show commands (continued)

Monitor commands	Corresponding show command page reference
monitor ports stats dhcp [<ports>]	page 200
monitor ports stats interface main [<ports>]	page 136
monitor ports stats interface extended [<ports>]	page 137
monitor ports stats interface utilization [<ports>]	page 307
monitor ports stats ospf main [<ports>]	page 235
monitor ports stats ospf extended [<ports>]	page 236
monitor ports stats routing [<ports>]	page 249
monitor ports stats stg [<ports>]	page 156
monitor ports stats vrrp extended [<ports>]	page 243
monitor ports stats vrrp main [<ports>]	page 243

Figure 196 shows output for the **monitor mlt stats interface utilization** command.

Figure 196 monitor mlt stats interface utilization command output

```
                        MLT INTERFACE UTILIZATION
Monitor Interval: 5sec | Monitor Duration: 300sec
MLT_ID     IN_OCTETS   OUT_OCTETS IN_UTIL(%) OUT_UTIL(%)
--------------------------------------------------------------------------------
1          5137408     17798464   0          0
2          0           0          0          0
3          0           0          0          0
4          0           0          0          0
7          5137536     17798528   0          0
8          0           0          0          0
```

Figure 197shows output for the **monitor ports stats interface utilization** command.

Figure 197 monitor ports stats interface utilization command output

```
                        PORT INTERFACE UTILIZATION
Monitor Interval: 5sec | Monitor Duration: 300sec

PORT_NUM IN_OCTETS  OUT_OCTETS IN_UTIL(%) OUT_UTIL(%)
--------------------------------------------------------------------------------
3/1      111613923  9326818    0          0
3/2      0          0          0          0
3/3      0          0          0          0
3/4      0          0          0          0
3/5      0          0          0          0
3/6      0          0          0          0
3/7      0          0          0          0
3/8      0          0          0          0
3/9      5141376    17811904   0          0
3/10     5141248    17811840   0          0
3/11     0          0          0          0
3/12     0          0          0          0
3/13     54179469954 4969856    10         0
3/14     0          0          0          0
3/15     0          0          0          0
3/16     0          0          0          0
```

Appendix A
CLI command list

Caution: Nortel Networks does not recommend or support IP Multicast with IGMP or DVMRP on the Passport 1000 platform.

This appendix provides an alphabetic list of CLI commands, with approximate page references for the beginning pages of further explanations. Commands listed in boldface type in Table 14 indicate commands that are new or revised. Commands that were in the previous release, or that have changed in syntax or in position in the command tree but add no new functionality, are listed in normal type.

Note: This information is presented for reference only and should not be considered an exact representation.

Table 14 CLI command list

command	Page No.
syntax back	page 78
boot [<devfile>] [config <value>] [ip <value>] [file <value>] [-y] box	page 79

Table 14 CLI command list (continued)

command	Page No.
clear ip arp ports <port> clear ip arp vlan <vid> clear ip route ports <port> clear ip route vlan <vid> clear igmp-snoop groups [<vid>] clear igmp-snoop mrouter [<vid>] clear ports stats [<ports>]	page 80
config cli banner add <string> **config cli banner default banner <true/false>** **config cli banner delete** **config cli banner info** **config cli defaultlogin <true|false>** **config cli defaultpassword <true|false>** **config cli loginprompt <string>** config cli monitor duration <integer> config cli monitor info	page 101
config cli monitor interval <integer> config cli more <true|false> **config cli motd add <string>** **config cli motd displaymotd <true/false>** **config cli motd delete** **config cli motd info** **config cli passwordprompt <string>**	page 101

Table 14 CLI command list (continued)

command	Page No.
config cli password info config cli password ro <username> [<password>] config cli password l1 <username> [<password>] config cli password l2 <username> [<password>] config cli password l3 <username> [<password>] config cli password rw <username> [<password>] config cli password rwa <username> [<password>] config cli prompt <prompt> config cli rlogin-sessions <nsessions> config cli screenlines <nlines> config cli telnet-sessions <nsessions> config cli timeout <seconds>	page 104
config ethernet <ports> auto-negotiate <enable|disable> config ethernet <ports> default-vlan-id <vid> config ethernet <ports> duplex <half|full> config ethernet <ports> high-priority <true|false> config ethernet <ports> info config ethernet <ports> ip arp-response disable config ethernet <ports> ip arp-response enable config ethernet <ports> ip arp-response info	page 127
config ethernet <ports> ip create <ipaddr/mask> config ethernet <ports> ip create-brouter <ipaddr/mask> <tag-id> config ethernet <ports> ip delete <ipaddr>	page 185
config ethernet <ports> ip dhcp-relay broadcast <enable|disable> config ethernet <ports> ip dhcp-relay disable config ethernet <ports> ip dhcp-relay enable config ethernet <ports> ip dhcp-relay info config ethernet <ports> ip dhcp-relay max-hop <max-hop> config ethernet <ports> ip dhcp-relay min-sec <min-sec> config ethernet <ports> ip dhcp-relay mode <mode>	page 198

Table 14 CLI command list (continued)

command	Page No.
config ethernet <ports> ip dvmrp enable config ethernet <ports> ip dvmrp disable config ethernet <ports> ip dvmrp info config ethernet <ports> ip dvmrp metric <cost>	page 254
config ethernet <ports> ip directed-broadcast disable **config ethernet <ports> ip directed-broadcast enable** **config ethernet <ports> ip directed-broadcast info**	page 185
config ethernet <ports> ip l3-igmp info config ethernet <ports> ip l3-igmp last-memb-query-int <seconds> config ethernet <ports> ip l3-igmp query-interval <seconds>	page 260
config ethernet <ports> ip l3-igmp query-max-resp <seconds> config ethernet <ports> ip l3-igmp robustval <integer> config ethernet <ports> ip l3-igmp version <integer> config ethernet <ports> ip info **config ethernet <ports> ip ospf enable** config ethernet <ports> ip ospf advertise-when-down <enable|disable> **config ethernet <ports> ip ospf disable** config ethernet <ports> ip ospf area <ipaddr> config ethernet <ports> ip ospf authentication-key <string> config ethernet <ports> ip ospf authentication-type <auth-type> config ethernet <ports> ip ospf dead-interval <seconds> config ethernet <ports> ip ospf hello-interval <seconds>	page 232
config ethernet <ports> ip ospf info config ethernet <ports> ip ospf metric <cost> config ethernet <ports> ip ospf priority <integer> config ethernet <ports> ip proxy disable config ethernet <ports> ip proxy enable config ethernet <ports> ip proxy info	page 192

Table 14 CLI command list (continued)

command	Page No.
config ethernet <ports> ip rip advertise-when-down <enable|disable> config ethernet <ports> ip rip auto-aggr <enable|disable> config ethernet <ports> ip rip default-listen <enable|disable> config ethernet <ports> ip rip default-supply <enable|disable> config ethernet <ports> ip rip disable config ethernet <ports> ip rip enable config ethernet <ports> ip rip info config ethernet <ports> ip rip listen <enable|disable> config ethernet <ports> ip rip manual trigger config ethernet <ports> ip rip poison <enable|disable> config ethernet <ports> ip rip supply <enable|disable> config ethernet <ports> ip rip trigger <enable|disable>	page 211
config ethernet <ports> ip traffic-filter default-action forward config ethernet <ports> ip traffic-filter default-action drop config ethernet <ports> ip traffic-filter default-action info config ethernet <ports> ip traffic-filter add set <value> config ethernet <ports> ip traffic-filter create config ethernet <ports> ip traffic-filter delete config ethernet <ports> ip traffic-filter disable config ethernet <ports> ip traffic-filter enable config ethernet <ports> ip traffic-filter info config ethernet <ports> ip traffic-filter remove set <value>	page 301
config ethernet <ports> ip vrrp <vrid> action <action choice> config ethernet <ports> ip vrrp <vrid> address <ipaddr> config ethernet <ports> ip vrrp <vrid> adver-int <seconds> config ethernet <ports> ip vrrp <vrid> critical-ip <ipaddr> config ethernet <ports> ip vrrp <vrid> delete config ethernet <ports> ip vrrp <vrid> disable config ethernet <ports> ip vrrp <vrid> enable **config ethernet <ports> ip vrrp <vrid> holddown-timer <seconds>** config ethernet <ports> ip vrrp <vrid> info config ethernet <ports> ip vrrp <vrid> priority <prio>	page 241

Table 14 CLI command list (continued)

command	Page No.
config ethernet <ports> lock <true|false> **config ethernet <ports> name <name>** **config ethernet <ports> oversize-frame <enable|disable>** config ethernet <ports> preferred-phy <left|right> config ethernet <ports> speed <10|100> config ethernet <ports> state <enable|disable|test>	page 127
config ethernet <ports> stg <sid> faststart <enable|disable> config ethernet <ports> stg <sid> info config ethernet <ports> stg <sid> pathcost <intval> config ethernet <ports> stg <sid> priority <intval> config ethernet <ports> stg <sid> stp <enable|disable>	page 151
config ethernet <ports> tagged-frames-discard <enable|disable> config ethernet <ports> perform-tagging <enable|disable> config ethernet <ports> untagged-frames-discard <enable|disable>	page 127
config ethernet <ports> unknown-mac-discard activation <enable|disable> **config ethernet <ports> unknown-mac-discard add-allow-mac <mac> <none|monitor> <low|high>** **config ethernet <ports> unknown-mac-discard activation <enable|disable>** **config ethernet <ports> unknown-mac-discard autolearn <enable|disable>** **config ethernet <ports> unknown-mac-discard autolearn-mode <one-shot|continuous>** **config ethernet <ports> unknown-mac-discard default-autolearn-monitor <none|monitor>** **config ethernet <ports> unknown-mac-discard default-autolearn-priority <low|high>** **config ethernet <ports> unknown-mac-discard info** **config ethernet <ports> unknown-mac-discard lock-autolearn-mac <enable|disable>** **config ethernet <ports> unknown-mac-discard remove-allow-mac <mac>** **config ethernet <ports> unknown-mac-discard violation-downport <enable|disable>** **config ethernet <ports> unknown-mac-discard violation-logging <enable|disable>** **config ethernet <ports> unknown-mac-discard violation-sendtrap <enable|disable>**	page 140
config info	page 110

Table 14 CLI command list (continued)

command	Page No.
config ip arp add ports <value> ip <value> mac <value> [vlan <value>] config ip arp aging <seconds> config ip arp delete <ipaddr> config ip arp info	page 189
config ip arp static-mcastmac add mac <value> ip <value> vlan <value> [ports <value>] [mlt <value>] **config ip arp static-mcastmac delete <ipaddr>** **config ip arp static-mcastmac info**	page 190
config ip default-ttl <seconds>	page 178
config ip dhcp-relay create-fwd-path agent <value> server <value> [mode <value>] [state <value>] config ip dhcp-relay enable-fwd-path agent <value> server <value> config ip dhcp-relay delete-fwd-path agent <value> server <value> config ip dhcp-relay disable-fwd-path agent <value> server <value> config ip dhcp-relay info config ip dhcp-relay mode <mode> agent <value> server <value>	page 197
config ip diffserv and-mask <integer> **config ip diffserv info** **config ip diffserv or-rule1 <integer>** **config ip diffserv or-rule2 <integer>** **config ip diffserv or-rule3 <integer>** **config ip diffserv tos-priority enable** **config ip diffserv tos-threshold <integer>**	page 182

Table 14 CLI command list (continued)

command	Page No.
config ip dvmrp disable config ip dvmrp enable config ip dvmrp info config ip dvmrp interface <ipaddr> disable config ip dvmrp interface <ipaddr> enable config ip dvmrp interface <ipaddr> info config ip dvmrp interface <ipaddr> metric <cost> config ip dvmrp update-interval <integer> config ip dvmrp triggered-update-interval <integer> config ip dvmrp leaf-timeout <integer> config ip dvmrp nbr-timeout <integer> config ip dvmrp nbr-probe-interval <integer>	page 249
config ip forwarding disable config ip forwarding enable config ip forwarding info	page 178
config ip l3-igmp info config ip l3-igmp interface <ipaddr> info config ip l3-igmp interface <ipaddr> last-memb-query-int <seconds> config ip l3-igmp interface <ipaddr> query-interval <seconds> config ip l3-igmp interface <ipaddr> query-max-resp <integer> config ip l3-igmp interface <ipaddr> robustval <integer> config ip l3-igmp interface <ipaddr> version <integer>	page 257
config ip info	page 257
config ip ipflow create src-ip <value> src-port <value> dst-ip <value> dst-port <value> protocol <value> config ip ipflow delete src-ip <value> src-port <value> dst-ip <value> dst-port <value> protocol <value> config ip ipflow info	page 278
config ip mroute info config ip mroute interface <ipaddr> ttl info config ip mroute interface <ipaddr> ttl <ttl>	page 178

Table 14 CLI command list (continued)

command	Page No.
config ip ospf admin-state <enable|disable>	page 218
config ip ospf area <area> create config ip ospf area <area> delete config ip ospf area <area> import-summaries <true|false> config ip ospf area <area> info config ip ospf area <area> nssa <true|false> config ip ospf area <area> range <ipaddr/mask> create advertise-mode <value> lsa-type <value> config ip ospf area <area> range <ipaddr/mask> delete config ip ospf area <area> range <ipaddr/mask> info config ip ospf area <area> stub <true|false> config ip ospf area <area> stub-metric <stub-metric> config ip ospf area <area> virtual-interface <nbr> authentication-key <authentication-key> config ip ospf area <area> virtual-interface <nbr> authentication-type <auth-type> config ip ospf area <area> virtual-interface <nbr> create config ip ospf area <area> virtual-interface <nbr> dead-interval <seconds> config ip ospf area <area> virtual-interface <nbr> delete config ip ospf area <area> virtual-interface <nbr> delete-message-digest-key <md5-key-id> config ip ospf area <area> virtual-interface <nbr> hello-interval <seconds> config ip ospf area <area> virtual-interface <nbr> info config ip ospf area <area> virtual-interface <nbr> add-message-digest-key <md5-key-id> md5-key <value> config ip ospf area <area> virtual-interface <nbr> retransmit-interval <seconds> config ip ospf area <area> virtual-interface <nbr> transit-delay <seconds> config ip ospf as-boundary-router <enable|disable|delete>	page 222
config ip ospf auto-vlink <enable|disable|delete> config ip ospf default-metric [ethernet <value>] [fast-ethernet <value>] [gig-ethernet <value>] config ip ospf disable config ip ospf enable config ip ospf holddown <seconds>	page 218

Table 14 CLI command list (continued)

command	Page No.
config ip ospf host-route <ipaddr> create config ip ospf host-route <ipaddr> delete config ip ospf host-route <ipaddr> info config ip ospf host-route <ipaddr> metric <metric> config ip ospf info	page 218
config ip ospf interface <ipaddr> admin-status <enable|disable> config ip ospf interface <ipaddr> area <area> config ip ospf interface <ipaddr> authentication-key <authentication-key> config ip ospf interface <ipaddr> authentication-type <auth-type> config ip ospf interface <ipaddr> dead-interval <seconds> config ip ospf interface <ipaddr> delete-message-digest-key <md5-key-id> config ip ospf interface <ipaddr> hello-interval <seconds> config ip ospf interface <ipaddr> info config ip ospf interface <ipaddr> add-message-digest-key <md5-key-id> md5-key <value> config ip ospf interface <ipaddr> metric <metric> config ip ospf interface <ipaddr> poll-interval <seconds> config ip ospf interface <ipaddr> priority <priority> config ip ospf interface <ipaddr> retransmit-interval <seconds> config ip ospf interface <ipaddr> transit-delay <seconds>	page 221
config ip ospf router-id <ipaddr> config ip ospf trap <enable|disable|delete>	page 219
config ip policy info config ip policy netlist <listid> add-network <ipaddr/mask> config ip policy netlist <listid> create config ip policy netlist <listid> delete config ip policy netlist <listid> info config ip policy netlist <listid> name <name>	page 280
config ip policy netlist <listid> remove-network <ipaddr/mask>	page 281

Table 14 CLI command list (continued)

command	Page No.
config ip policy ospf accept <pid> action <accept|ignore> config ip policy ospf accept <pid> create config ip policy ospf accept <pid> delete config ip policy ospf accept <pid> disable config ip policy ospf accept <pid> enable config ip policy ospf accept <pid> exact-net-list <netlist id> config ip policy ospf accept <pid> ext-metric-type <type1|type2> config ip policy ospf accept <pid> info config ip policy ospf accept <pid> inject-net-list <netlist id> config ip policy ospf accept <pid> name <string> config ip policy ospf accept <pid> precedence <precedence> config ip policy ospf accept <pid> range-net-list <netlist id>	page 282
config ip policy ospf announce <pid> action <announce|ignore> config ip policy ospf announce <pid> add-route-source <direct|static|rip|any> config ip policy ospf announce <pid> advertise-netlist <netlist id> config ip policy ospf announce <pid> create config ip policy ospf announce <pid> delete config ip policy ospf announce <pid> disable config ip policy ospf announce <pid> enable config ip policy ospf announce <pid> exact-netlist <netlist id> config ip policy ospf announce <pid> ext-metric <ext-metric> config ip policy ospf announce <pid> ext-metric-type <type1|type2> config ip policy ospf announce <pid> info config ip policy ospf announce <pid> name <string> config ip policy ospf announce <pid> precedence <precedence> config ip policy ospf announce <pid> range-netlist <netlist id> config ip policy ospf announce <pid> remove-route-source <direct|static|rip|any> config ip policy ospf announce <pid> rip-gateway-list <addrlist id> config ip policy ospf announce <pid> rip-interface-list <addrlist id>	page 284
config ip policy ospf apply-accept config ip policy ospf apply-announce	page 282
config ip policy ospf info	page 282

Table 14 CLI command list (continued)

command	Page No.
config ip policy rip accept <pid> action <accept|ignore> config ip policy rip accept <pid> apply-mask <ipmask> config ip policy rip accept <pid> create config ip policy rip accept <pid> delete config ip policy rip accept <pid> disable config ip policy rip accept <pid> enable config ip policy rip accept <pid> exact-netlist <netlist id> config ip policy rip accept <pid> info config ip policy rip accept <pid> inject-netlist <netlist id> config ip policy rip accept <pid> name <string> config ip policy rip accept <pid> precedence <precedence> config ip policy rip accept <pid> range-netlist <netlist id> config ip policy rip accept <pid> rip-gateway-list <addrlist id> config ip policy rip accept <pid> rip-interface-list <listid>	page 286
config ip policy rip announce <pid> action <announce|ignore> **config ip policy rip announce <pid> add-route-source <direct|static|rip|ospf|any>** config ip policy rip announce <pid> advertise-netlist <netlist id> config ip policy rip announce <pid> create config ip policy rip announce <pid> delete config ip policy rip announce <pid> disable config ip policy rip announce <pid> enable config ip policy rip announce <pid> exact-netlist <netlist id> config ip policy rip announce <pid> info config ip policy rip announce <pid> name <string> config ip policy rip announce <pid> ospf-router-id-list <addrlist id> config ip policy rip announce <pid> ospf-route-type <type1|type2|external|internal|any> config ip policy rip announce <pid> outbound-interface-list <addrlist id> config ip policy rip announce <pid> precedence <precedence> config ip policy rip announce <pid> range-netlist <netlist id> config ip policy rip announce <pid> remove-route-src <direct|static|rip|ospf|any> config ip policy rip announce <pid> rip-gateway-list <addrlist id> config ip policy rip announce <pid> rip-interface-list <addrlist id> config ip policy rip announce <pid> rip-metric <rip-metric>	page 287
config ip policy rip info	page 285

Table 14 CLI command list (continued)

command	Page No.
config ip route delete <ipaddr/mask> **config ip route delete info**	page 178
config ip route-discovery disable config ip route-discovery enable config ip route-discovery info	page 178
config ip rip disable config ip rip domain <ipaddr> <value> config ip rip enable config ip rip holddown <seconds> config ip rip info config ip rip updatetime <seconds> config ip rip receive <ipaddr> mode <value> config ip rip send <ipaddr> mode <value>	page 208
config ip static-route create <ipaddr|mask> next-hop <value> cost <value> **config ip static-route delete <ipaddr|mask> next-hop <value>** **config ip static-route disable <ipaddr|mask> next-hop <value>** **config ip static-route enable <ipaddr|mask> next-hop <value>** config ip static-route info	page 178

Table 14 CLI command list (continued)

command	Page No.
config ip traffic-filter clear-stats [<fid>] **config ip traffic-filter create destination <value> [src-ip <value>] [id <id>]** **config ip traffic-filter create global [src-ip <value>] [dst-ip <value>] [id <id>]** config ip traffic-filter create info **config ip traffic-filter create source <value> [dst-ip <value>] [id <id>**] config ip traffic-filter filter <fid> action mode <default|forward|drop> config ip traffic-filter filter <fid> action info config ip traffic-filter filter <fid> action mirror <enable|disable> **config ip traffic-filter filter <fid> action high-priority <enable|disable>** config ip traffic-filter filter <fid> action tcp-connect <enable|disable> config ip traffic-filter filter <fid> action use-packet-limit <enable|disable> config ip traffic-filter filter <fid> delete config ip traffic-filter filter <fid> log-stats <enable|disable> config ip traffic-filter filter <fid> info config ip traffic-filter filter <fid> match dst-port <port> [dst-option <value>] config ip traffic-filter filter <fid> match info config ip traffic-filter filter <fid> match packet-limit <pktlimit> config ip traffic-filter filter <fid> match protocol <protocoltype> config ip traffic-filter filter <fid> match src-port <port> [src-option <value>]	page 295
config ip traffic-filter filter <fid> modify info config ip traffic-filter filter <fid> modify diffserv-rule <none|rule1|rule2|rule3> config ip traffic-filter filter <fid> modify vlan-tag-priority <vlan-priority-number> config ip traffic-filter filter <fid> name <name> config ip traffic-filter global-set <gsetid> add-filter <fid> config ip traffic-filter global-set <gsetid> create [name <value>] config ip traffic-filter global-set <gsetid> delete config ip traffic-filter global-set <gsetid> info config ip traffic-filter global-set <gsetid> remove-filter <fid> config ip traffic-filter info config ip traffic-filter log-interval<seconds> config ip traffic-filter set <setid> add-filter <fid> config ip traffic-filter set <setid> create [name <value>] config ip traffic-filter set <setid> delete config ip traffic-filter set <setid> info config ip traffic-filter set <setid> remove-filter <fid>	page 295

Table 14 CLI command list (continued)

command	Page No.
config ip udpfwd info config ip udpfwd interface <ipaddr> create <fwdlistid> config ip udpfwd interface <ipaddr> delete config ip udpfwd interface <ipaddr> info config ip udpfwd interface <ipaddr> maxttl <maxttl> config ip udpfwd interface <ipaddr> udpportfwdlist <fwdlistid> config ip udpfwd portfwdlist <fwdlistid> add-portfwd <udpport> <ipaddr> config ip udpfwd portfwdlist <fwdlistid> create config ip udpfwd portfwdlist <fwdlistid> delete config ip udpfwd portfwdlist <fwdlistid> info config ip udpfwd portfwdlist <fwdlistid> name <name> config ip udpfwd portfwdlist <fwdlistid> remove-portfwd <udpport> <ipaddr> config ip udpfwd protocol <updport> create <protoname> config ip udpfwd protocol <updport> delete config ip udpfwd protocol <updport> info	page 203
config ipx forwarding disable [<IPX-network-number>] config ipx forwarding enable [<IPX-network-number>] config ipx forwarding info config ipx info	page 264
config ipx rip default-delay <delay-timer> **config ipx rip default-hold-multiplier <age-multiplier>** config ipx rip default-interval <interval-timer> config ipx rip info	page 269
config ipx rip age-multiplier <IPX-network-number> <age-multiplier> **config ipx rip state <IPX-network-number> <on|off>** config ipx rip update-delay <IPX-network-number> <delay-timer> config ipx rip update-interval <IPX-network-number> <interval-timer>	page 270

Table 14 CLI command list (continued)

command	Page No.
config ipx sap age-multiplier <IPX-network-number> <age-multiplier> config ipx sap create <service-type> <service-name> <ipxhost> <socket-number> <hop-count> config ipx sap delete <service-name> config ipx sap default-delay <delay-timer> config ipx sap default-hold-multiplier <age-multiplier> config ipx sap default-interval <interval-timer> config ipx sap hold-multiplier <IPX-network-number> <hold-multiplier> config ipx sap info config ipx sap update-delay <IPX-network-number> <delay-timer> config ipx sap update-interval <IPX-network-number> <interval-timer>	page 271 and page 272
config ipx set info config ipx set max-route <max_entries> config ipx set max-sap <max_entries> config ipx set max-static-route <max_entries> config ipx set max-static-sap <max_entries>	page 267
config ipx static-route info config ipx static-route create <IPX-network-number> <nexthop> <hop-count> <tick-count> config ipx static-route delete <IPX-network-number>	page 268
config log clear config log info config log level [<level>] config log screen [<setting>] config log write <str>	page 106
config mirror inport1 <port> <enable|disable> config mirror inport2 <port> <enable|disable> config mirror outport <port> <enable|disable> config mirror saveconfig <true|false>	page 145

Table 14 CLI command list (continued)

command	Page No.
config radius attribute-value <value> **config radius enable <true/false>** **config radius info** **config radius maxserver <value>** **config radius server create <ipaddr> secret <value> [port <value>] [priority <value>] [retry <value>] [timeout <value>] [enable <value>]** **config radius server delete <ipaddr>** **config radius server info** **config radius server set <ipaddr> [secret<value>] [ports <value>] [priority <value>] [retry <value>] [timeout <value>] [enable <value>]**	page 142
config mlt <mid> add info config mlt <mid> add ports <ports> config mlt <mid> add vlan <vid> config mlt <mid> create config mlt <mid> delete config mlt <mid> info config mlt <mid> name <string> config mlt <mid> remove info config mlt <mid> remove ports <ports> config mlt <mid> remove vlan <vid> config mlt <mid> perform tagging <enable|disable>	page 146
config rmon disable config rmon enable config rmon info	page 109
config setdate	page 110

Table 14 CLI command list (continued)

command	Page No.
config stg <sid> add ports <value> **config stg <sid> create [<ports>] [mac <value>] [vlan <value>]** config stg <sid> delete config stg <sid> forward-delay <timeval> config stg <sid> group-stp <enable|disable> config stg <sid> hello-interval <timeval> config stg <sid> info config stg <sid> max-age <timeval> config stg <sid> priority <number> config stg <sid> remove ports <value> config stg <sid> trap-stp <enable|disable>	page 150
config sys access-policy enable <true|false> config sys access-policy info config sys access-policy policy <pid> accesslevel <level> config sys access-policy policy <pid> create config sys access-policy policy <pid> delete config sys access-policy policy <pid> disable config sys access-policy policy <pid> enable config sys access-policy policy <pid> host <ipaddr> config sys access-policy policy <pid> info config sys access-policy policy <pid> mode <mode> config sys access-policy policy <pid> name <name> config sys access-policy policy <pid> network <addr/mask> config sys access-policy policy <pid> precedence <precedence> config sys access-policy policy <pid> service http <enable|disable> config sys access-policy policy <pid> service info config sys access-policy policy <pid> service rlogin <enable|disable> config sys access-policy policy <pid> service snmp <enable|disable> config sys access-policy policy <pid> service telnet <enable|disable> config sys access-policy policy <pid> username <string>	page 111
config sys diag aru-monitor <enable|disable> **config sys diag info**	
config sys info	page 110

Table 14 CLI command list (continued)

command	Page No.
config sys link-flap-detect auto-port-down <enable|disable> **config sys link-flap-detect frequency <frequency>** **config sys link-flap-detect info** **config sys link-flap-detect interval <interval>** **config sys link-flap-detect send-trap <enable|disable>**	page 122
config sys set action checkswinflash config sys set action checkswinpcmcia **config sys set action cpuswitchover [-y]** config sys set action getstandbycpuinfo config sys set action info config sys set action resetconsole **config sys set action resetcounters [-y]** config sys set action resetmodem config sys set action savetostandbynvram	page 114
config sys set boot <primary|secondary|tertiary> <choice> config sys set config <choice> config sys set contact <contact> config sys set eoc-mode <eocmode>	page 117
config sys set flags autoboot <true|false> config sys set flags factorydefault <true|false> config sys set flags switchportiso <true|false> config sys set flags debugmode <true|false> config sys set flags highpriomode <true|false> config sys set flags info	page 115

Table 14 CLI command list (continued)

command	Page No.
config sys set info config sys set location <location> config sys set name <prompt> config sys set portlock <on|off> config sys set sendtrap <true|false> **config sys set snmp community <ro|11|l2|l3|rw|rwa> <commstr>** config sys set snmp info config sys set snmp trap-recv <ipaddr> <v1|v2c> <commstr> config sys set topology <on|off>	page 117
config sys syslog host <id> address <ipaddr> config sys syslog host <id> create config sys syslog host <id> delete config sys syslog host <id> facility <facility> config sys syslog host <id> host <enable|disable> config sys syslog host <id> info config sys syslog host <id> mapinfo <level> config sys syslog host <id> mapwarning <level> config sys syslog host <id> maperror <level> config sys syslog host <id> mapfatal <level> config sys syslog host <id> severity <info|warning|error|fatal> [<info|warning|error|fatal>] config sys syslog host <id> udp-port <port> config sys syslog info config sys syslog max-hosts <maxhost> config sys syslog state <enable|disable>	page 123
config sys telnet-client <enable|disable> **config sys tftp-server <enable|disable>**	page 111

Table 14 CLI command list (continued)

command	Page No.
config vlan <vid> action <action choice> config vlan <vid> agetime <10..100000> config vlan <vid> create byport <sid> [name <value>] config vlan <vid> create byprotocol <sid> <ip|ipx802dot3|ipx802dot2|ipxSnap|ipxEthernet2|appleTalk|decLat|decOther|sna802 dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp> [pid] [name <value>] config vlan <vid> create byipsubnet <sid> <ipaddr/mask> [name <value>] config vlan <vid> create bysrcmac <sid> [name <value>] config vlan <vid> create info config vlan <vid> delete	page 159
config vlan <vid> fdb-entry aging-time <seconds> config vlan <vid> fdb-entry flush config vlan <vid> fdb-entry info config vlan <vid> fdb-entry monitor <mac> status <value> <true|false> config vlan <vid> fdb-entry priority <mac> status <value> <high|low> config vlan <vid> fdb-filter add <mac> port <value> config vlan <vid> fdb-filter info config vlan <vid> fdb-filter notallowfrom add <mac> port <value> config vlan <vid> fdb-filter notallowfrom info config vlan <vid> fdb-filter notallowfrom remove <mac> port <value> config vlan <vid> fdb-filter remove <mac> config vlan <vid> fdb-static add <mac> port <value> config vlan <vid> fdb-static info config vlan <vid> fdb-static remove <mac>	page 165
config vlan <vid> highpriority <true|false>	page 159

Table 14 CLI command list (continued)

command	Page No.
config vlan <vid> igmp-snoop access-list <GroupAddress> create <HostAddress> <HostMask> <denyRX|denyTX|denyBoth> config vlan <vid> igmp-snoop access-list <GroupAddress> delete <HostAddress> <HostMask> config vlan <vid> igmp-snoop access-list <GroupAddress> info config vlan <vid> igmp-snoop access-list <GroupAddress> mode <HostAddress> <HostMask> <denyRX|denyTX|denyBoth> config vlan <vid> igmp-snoop info config vlan <vid> igmp-snoop mrouter <ports> config vlan <vid> igmp-snoop query-interval <seconds> config vlan <vid> igmp-snoop report-proxy <enable|disable> config vlan <vid> igmp-snoop robust-value <integer> **config vlan <vid> igmp-snoop sender flush [<Group/IP Address>] [<ports>] [<Host/IP Address>]** config vlan <vid> igmp-snoop sender info config vlan <vid> igmp-snoop state <enable|disable> config vlan <vid> igmp-snoop static-members <GroupAddress> add <ports> <static|blocked> config vlan <vid> igmp-snoop static-members <GroupAddress> create <ports> <static|blocked> config vlan <vid> igmp-snoop static-members <GroupAddress> delete config vlan <vid> igmp-snoop static-members <GroupAddress> info config vlan <vid> igmp-snoop static-members <GroupAddress> remove <ports> <static|blocked>	page 168
config vlan <vid> info	page 159
config vlan <vid> ip create <ipaddr/mask> config vlan <vid> ip delete <ipaddr>	page 186

Table 14 CLI command list (continued)

command	Page No.
config vlan <vid> ip dhcp-relay broadcast <enable|disable> config vlan <vid> ip dhcp-relay disable config vlan <vid> ip dhcp-relay enable config vlan <vid> ip dhcp-relay info config vlan <vid> ip dhcp-relay max-hop <max-hop> config vlan <vid> ip dhcp-relay min-sec <min-sec> config vlan <vid> ip dhcp-relay mode <mode> config vlan <vid> ip dhcp-relay relay agent <value> server <value> mode <value> config vlan <vid> ip dhcp-relay to agent <value> server <value> state <value>	page 201
config vlan <vid> ip directed-broadcast disable **config vlan <vid> ip directed-broadcast enable** **config vlan <vid> ip directed-broadcast info**	page 186
config vlan <vid> ip dvmrp enable config vlan <vid> ip dvmrp disable config vlan <vid> ip dvmrp info config vlan <vid> ip dvmrp metric <cost>	page 256
config vlan <vid> ip l3-igmp info config vlan <vid> ip l3-igmp last-memb-query-int <seconds> config vlan <vid> ip l3-igmp query-interval <seconds> config vlan <vid> ip l3-igmp query-max-resp <seconds> config vlan <vid> ip l3-igmp robustval <integer> config vlan <vid> ip l3-igmp version <integer>	page 261
config vlan <vid> ip info	page 186

Table 14 CLI command list (continued)

command	Page No.
config vlan <vid> ip ospf advertise-when-down <enable|disable> config vlan <vid> ip ospf enable config vlan <vid> ip ospf disable config vlan <vid> ip ospf area <ipaddr> config vlan <vid> ip ospf authentication-key <string> config vlan <vid> ip ospf authentication-type <auth-type> config vlan <vid> ip ospf dead-interval <seconds> config vlan <vid> ip ospf hello-interval <seconds> config vlan <vid> ip ospf info config vlan <vid> ip ospf metric <cost> config vlan <vid> ip ospf priority <integer>	page 237
config vlan <vid> ip proxy disable config vlan <vid> ip proxy enable config vlan <vid> ip proxy info config vlan <vid> ip resp disable config vlan <vid> ip resp enable config vlan <vid> ip resp info	page 194
config vlan <vid> ip rip advertise-when-down <enable|disable> config vlan <vid> ip rip auto-aggr <enable|disable> config vlan <vid> ip rip default-listen <enable|disable> config vlan <vid> ip rip default-supply <enable|disable> config vlan <vid> ip rip disable config vlan <vid> ip rip enable config vlan <vid> ip rip info config vlan <vid> ip rip listen <enable|disable> config vlan <vid> ip rip manualtrigger config vlan <vid> ip rip poison <enable|disable> config vlan <vid> ip rip supply <enable|disable> config vlan <vid> ip rip trigger <enable|disable>	page 215

Table 14 CLI command list (continued)

command	Page No.
config vlan <vid> ip vrrp <vrid> action <action choice> config vlan <vid> ip vrrp <vrid> address <ipaddr> config vlan <vid> ip vrrp <vrid> adver-int <seconds> config vlan <vid> ip vrrp <vrid> critical-ip <ipaddr> config vlan <vid> ip vrrp <vrid> delete config vlan <vid> ip vrrp <vrid> disable config vlan <vid> ip vrrp <vrid> enable **config vlan <vid> ip vrrp <vrid> holddown-timer <seconds>** config vlan <vid> ip vrrp <vrid> info config vlan <vid> ip vrrp <vrid> priority <prio>	page 244
config vlan <vid> ipx create <IPX-network-number> [encapsulation] config vlan <vid> ipx delete <IPX-network-number> config vlan <vid> ipx info	page 266
config vlan <vid> name <vname> config vlan <vid> ports add <ports> [member <value>] config vlan <vid> ports info config vlan <vid> ports remove <ports> [member <value>] config vlan <vid> srcmac add <macaddr> config vlan <vid> srcmac info config vlan <vid> srcmac remove <macaddr>	page 159
config vlan <vid> static-mcastmac add mac <value> [ports <value>] [mlt <value>] **config vlan <vid> static-mcastmac add-mlt <mid> mac <value>** **config vlan <vid> static-mcastmac add-ports <ports> mac <value>** **config vlan <vid> static-mcastmac delete mac <value>** **config vlan <vid> static-mcastmac delete-mlt <mid> mac <value>** **config vlan <vid> static-mcastmac delete-ports <ports> mac <value>** **config vlan <vid> static-mcastmac info**	page 174

Table 14 CLI command list (continued)

command	Page No.
config web-server disable config web-server enable config web-server info config web-server set info config web-server set password <ro|rw|rwa> <username> <passwd>	page 126
copy <srcdevfile> <destdevfile> [debug] [ip <value>]	page 88
cwc [..] date	page 78
delete <devfile> directory [<device>]	page 88
exit **format <device> [-y]** help [<command>] history login logout	page 78

Table 14 CLI command list (continued)

command	Page No.
monitor mlt error collision [<mid>] monitor mlt error main [<mid>] monitor mlt stats interface main [<mid>] monitor mlt stats interface utilization [<mid>] monitor ports error collision [<ports>] monitor ports error extented [<ports>] monitor ports error main [<ports>] monitor ports error ospf [<ports>] monitor ports stats bridging [<ports>] monitor ports stats dhcp [<ports>] monitor ports stats interface main [<ports>] monitor ports stats interface extended [<ports>] monitor ports stats interface utilization [<ports>] monitor ports stats ospf main [<ports>] monitor ports stats ospf extended [<ports>] monitor ports stats routing [<ports>] monitor ports stats stp [<ports>] **monitor ports stats vrrp extended [<ports>]** **monitor ports stats vrrp main [<ports>]**	page 305
ping <ipaddr> [<datasize>] [<count>] [-s] [-I <value>] [-t <value>] [-d] pingipx <ipxhost> [<count>] [-s] [-q] [-t <value<] pwc quit recover <device> **reset [-y]** rlogin <ipaddr> rsh <ipaddr> -l <value> <cmd> save [<devfile>] [standby]	page 78
show config [verbose]	page 97
show cli info show cli password show cli who	page 103

Table 14 CLI command list (continued)

command	Page No.
show ip arp info [<ip address>] [-s <value>]	page 191
show ip dhcp fwd-path show ip dhcp counters	page 197
show ip diffserv	page 184
show ip dvmrp info show ip dvmrp interface show ip dvmrp neighbor show ip dvmrp next-hop show ip dvmrp route	page 251
show ip flow	page 278
show ip forwarding show ip interface	page 180
show ip l3-igmp cache show ip l3-igmp group show ip l3-igmp interface	page 258
show ip mroute interface show ip mroute next-hop show ip mroute route	page 247

Table 14 CLI command list (continued)

command	Page No.
show ip ospf area **show ip ospf ase [metric-type <value>] [detail]** show ip ospf default-metric show ip ospf host-route show ip ospf ifstats [mismatch] show ip ospf info show ip ospf interface show ip ospf int-timers show ip ospf lsdb [area <value>] [lsatype <value>] [lsid <value>] [adv_rtr <value>] [detail] show ip ospf neighbors show ip ospf range show ip ospf stats	page 225
show ip policy addrlist info [id <value>]	page 289
show ip policy netlist info [id <value>]	page 290
show ip policy ospf accept info [id <value>] show ip policy ospf accept lists [id <value>] show ip policy ospf accept match network <value>	page 291
show ip policy ospf announce info [id <value>] show ip policy ospf announce lists [id <value>] show ip policy ospf announce match network <value>	page 292
show ip policy rip accept info [id <value>] show ip policy rip accept lists [id <value>] show ip policy rip accept match network <value>	page 293
show ip policy rip announce info [id <value>] show ip policy rip announce lists [id <value>] show ip policy rip announce match network <value>	page 294
show ip route-discovery	page 181

Table 14 CLI command list (continued)

command	Page No.
show ip rip info show ip rip interface [<ipaddr>] show ip route info [<ip address>] [-s <value>]	page 210
show ip traffic-filter active show ip traffic-filter destination [<fid>] show ip traffic-filter disabled [<ports>] show ip traffic-filter enabled [<ports>] show ip traffic-filter global [<fid>] show ip traffic-filter info global-list [<id>] show ip traffic-filter info list [<id>] show ip traffic-filter interface <ports> show ip traffic-filter log-interval show ip traffic-filter source [<fid>] show ip traffic-filter stats [<fid>]	page 301
show ip udpfwd interface info [<ipaddr>] show ip udpfwd portfwd info show ip udpfwd portfwdlist info [<fwdlistid>] show ip udpfwd protocol info	page 205
show ip vrrp info [<vrid>] [<ipaddr>] show ip vrrp stats <vrid> <ipaddr>	page 245
show ipx config [<IPX-network-number>] show ipx default show ipx route [<IPX-network-number>] [<IPX-network-number>] show ipx sap [<service-name>] show ipx stats <IPX-network-number>	page 273
show log file [tail] show log level	page 107

Table 14 CLI command list (continued)

command	Page No.
show mlt error collision [<mid>] show mlt error main [<mid>] show mlt info [<mid>] show mlt stats [<mid>]	page 147
show mirrorinfo	page 145
show ports error collision [<ports>] show ports error extented [<ports>] show ports error main [<ports>] show ports error ospf [<ports>]	page 129
show ports info all [<ports>] [by <value>] show ports info arp [<ports>] show ports info config [<ports>] show ports info dhcp [<ports>] show ports info dvmrp [<ports>] show ports info l3-igmp [<ports>] show ports info interface [<ports>] show ports info ip [<ports>] **show ports info name [<port>]** show ports info ospf [<ports>] show ports info rip [<ports>] show ports info stg main [<ports>] show ports info stg extended [<ports>] **show ports info unknown-mac-discard [<ports>]** show ports info vlans [<ports>] show ports info vrrp main [<ports>] show ports info vrrp extended [<ports>]	page 133

Table 14 CLI command list (continued)

command	Page No.
show ports stats bridging [<ports>] show ports stats dhcp [<ports>] show ports stats interface main [<ports>] show ports stats interface extended [<ports>] show ports stats ospf main [<ports>] show ports stats ospf extended [<ports>] show ports stats routing [<ports>] show ports stats stg [<ports>] show ports stats vrrp [<ports>]	page 135
show radius info **show radius server config** **show radius server stat**	page 142
show rmon	page 109
show stg info config [<sid>] show stg info status [<sid>]	page 152
show sys access-policy info [<polname>]	page 113
show sys community show sys diag info show sys info show sys perf show sys sw show sys syslog general-info show sys syslog host <id> info	page 119
show tech	page 100
show test artable show test fabric show test loopback [<ports>]	page 93

Table 14 CLI command list (continued)

command	Page No.
show trace file [tail] show trace level	page 95
show vlan info advance [<vid>] show vlan info all [<vid>] [by <value>]	page 161
show vlan info arp [<vid>] **show vlan info autolearn-mac** show vlan info basic [<vid>] show vlan info dhcp [<vid>]	page 194
show vlan info dvmrp [<vid>] show vlan info fdb-entry <vid>	page 162
show vlan info fdb-filter <vid> show vlan info igmp [<vid>] show vlan info ip [<vid>] show vlan info ipx [<vid>]	page 263
show vlan info manual-edit-mac	page 164
show vlan info ospf [<vid>] show vlan info ports [<vid>] show vlan info rip [<vid>] show vlan info snoop [<vid>]	page 217
show vlan info srcmac [<vid>] show vlan info fdb-static <vid> show vlan info vrrp main [<vid>] show vlan info vrrp extended [<vid>]	page 245

Table 14 CLI command list (continued)

command	Page No.
show vlan igmp-snoop access-list <vid> [<Group Address>] show vlan igmp-snoop all-access-list show vlan igmp-snoop groups [<vid>] show vlan igmp-snoop senders info [<vid>] show vlan igmp-snoop static [<vid>]	page 172
show web-server	page 126
squeeze <device> telnet [<ipaddr>]	page 78
test artable test fabric test loopback <ports> [<int|ext>] test stop artable test stop fabric test stop loopback <ports>	page 92
toplevel	page 78
trace clear trace level [<modid>] [<level>] trace off trace screen [<setting>] trace info [tail] traceroute <ipaddr> [<datasize>] [-m <value>] [-p <value>] [-q <value>] [-w <value>] [-v]	page 94

Appendix B
Port numbering and MAC address assignment

Caution: IP Multicast with IGMP and DVMRP is not supported on this platform.

This appendix explains how ports are numbered on the chassis. It also explains how MAC addresses are assigned to MAC entities in the Passport 1000 Series switch.

Port numbering

Some screens contain fields for selecting ports. A port number includes the slot location of the I/O module in the chassis, as well as the port's position in the I/O module. In the Passport 1200 Switch, slots are numbered from top to bottom. Figure 198 shows slot numbering for the Passport 1200 Switch.

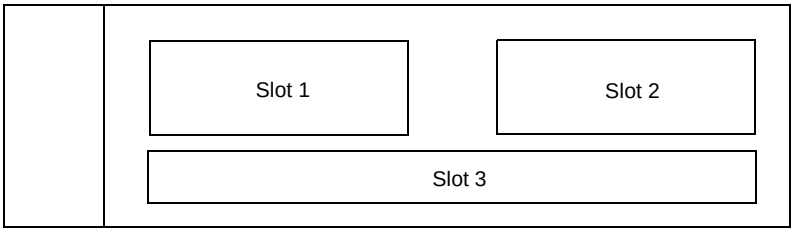
Figure 198 Passport 1200 slots

Power supply 1	I/O slot 1
	I/O slot 2
	I/O slot 3
	FB-SSF CPU board
Power supply 2	FB-SSF CPU board
	I/O slot 6
	I/O slot 7
	I/O slot 8

7814EA

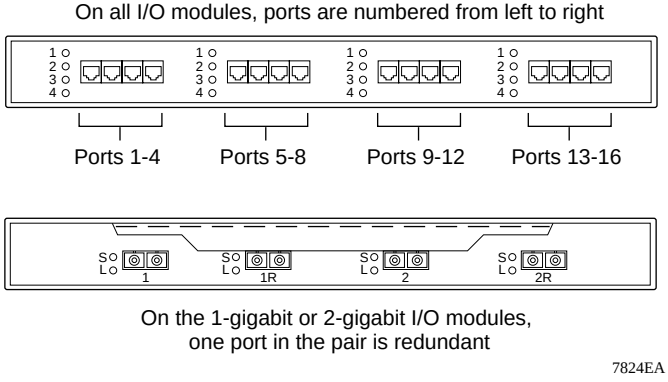
In the Passport 1100 Switch or Passport 1150 Switch, the modular slots are slots 1 and 2 and the internal ports belong to slot 3. Figure 199 shows how slots on a Passport 1100 chassis are numbered from left to right.

Figure 199 Passport 1100 slots



Ports in the chassis and in all modules are numbered from left to right. For example, the second port in an I/O module located in slot 1 is 1/2. Figure 200 shows port numbering on modules.

Figure 200 Port numbering on I/O modules



Use the slot and module examples in the figures as guides when you need help selecting ports in Passport Device Manager.

MAC address assignment

Understanding how MAC addresses are assigned is important when defining static ARP entries for IP addresses in the routing switch and when using a network analyzer to decode network traffic.

Base MAC address

A flash memory device holds a unique 48-bit base MAC address for the Passport 1000 Series switch. For the Passport 1200 chassis, the flash device is in the main chassis. For the Passport 1100 or 1150 chassis, the flash device is on the main board with the fixed ports.

For a given switch, the base MAC address format is:

```
xx xx xx yy yy 00
```

where:

xx xx xx is the IEEE organization identifier (for example, 00 0E 16).

yy yy is unique to the switch.

On switches with debug Ethernet ports, the base MAC address is used by this port.

The general form for a MAC addresses used by a particular switch is:

```
xx xx xx yy yy zz
```

where:

xx xx xx is the IEEE organization identifier (for example, 00 0E 16).

yy yy is unique to the switch.

zz is user specific.

From the general form, it is easy to see that each Passport 1000 Series switch is assigned a block of 256 48-bit MAC addresses from xx xx xx yy yy 00 through xx xx xx yy yy FF.

Physical MAC addresses

Physical MAC addresses are addresses assigned to the physical interfaces or ports visible on the device. The physical MAC addresses are used in the following types of frames:

- Spanning Tree Protocol BPDUs sent by the routing switch
- Frames to or from an isolated routing port's physical interface

BPDUs are sent using the physical MAC address as the source because identifying which physical port sent the BPDU is critical to how the Spanning Tree Protocol works. For isolated routing ports, the IP address is associated with the physical interface, so the physical MAC address is associated with the IP address.

The last byte of the MAC address (zz in the general form) for a physical interface depends on the slot and port number for the given interface. The basic scheme is that each slot is allocated 16 physical MAC addresses. If a board has fewer than 16 ports, some MAC addresses are unused. Table 15 lists the value for the last byte of the MAC address based on the slot and port number.

Table 15 Last byte of physical MAC address

	Port															
Slot	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**15**
1	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
2	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
3	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F
4	Not applicable—contains SSF module															
5	Not applicable—contains SSF module															
6	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F
7	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F
8	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F

Slots 4 and 5 do not have any MAC addresses assigned to them. Depending on which switch you are operating, slots 4 and 5 may not be present or hold the SSF modules. For example, a switch with the base MAC address 00 0E 16 11 00 00 has a physical MAC address for slot 3 port 6 (port 3/6) of 00 0E 16 11 00 25. This MAC address is seen as the source MAC address for any BPDUs sent out of this port. If port 3/6 is configured as an isolated routing port, ARP requests sent to the IP address of the isolated routing port will return this MAC address.

Virtual MAC addresses

Virtual MAC addresses are the addresses assigned to VLANs. A virtual MAC address is assigned to a VLAN when it is created. The MAC address for a VLAN IP address is the virtual MAC address assigned to the VLAN.

The range for the last byte of the virtual MAC addresses in hex is 81 through FF; that is, the most significant bit of the last byte is set to 1.

A virtual MAC address is assigned when a VLAN is created. The Default VLAN (VLAN ID 1) is always created; therefore, the last byte of the MAC address for VLAN 1 is always 81. For other VLANs, the MAC address assigned can be found in Device Manager (VLAN > VLAN > Advanced) or through the run-time CLI (**`show vlan info advance`** command).

Index

A

accept policy
OSPF 282
RIP 286
access levels 52
access policies 110
access-policy commands
configure 111
show 113
address lists 280
alphabetical list of commands 309
announce policy
OSPF 284
RIP 287
ARP commands
configure 188
IP 189
port 192
show 191
VLAN 194
ARU2 hardware 70
ARU3 hardware 70
authentication
RADIUS 142

B

base MAC address 345
boot command
Boot Monitor CLI 59
Run-Time CLI 79
boot configuration 36, 59
boot factory default 39
boot flash memory 40
Boot Monitor CLI
accessing 56
command list 56
definition 35, 55
Boot Monitor CLI commands
boot 59
choices 59
delete 60
device management 60
devices 59
directory 61
file management 60
flags 59
format 61
help 62
history 62
ip 63
log 61
ping 65
quit 67
recover 61
reset 59
save 59
show 59, 67
squeeze 61
tests 59
tftp 60
trace 61
boot monitor image file 42
boot options
internal flash 59
network 59
PCMCIA 59

skip 59
boot order, specifying 59
boot sequence 36
boot source, specifying 59

C

choices command 59
clear commands 80
CLI command list, alphabetical 309
CLI command tree 77
commands, config cli password 54
config cli commands 101
config cli management commands 101
config cli password commands 54, 104
config ip diffserv-rule commands 184
config ip filter commands 295
config ip ospf commands 219–225
config ip policy commands 279–289
config log commands 106
config mirror commands 145
config radius commands 142
config rmon commands 109
config setdate command 110
config sys access-policy commands 111–113
config web-server commands 126
configuration
default 39
files 42
loading 38
configuration, RADIUS 144
conventions 28
conventions, text 28
copy command 48, 60, 88
customer support 32

D

date command 81
defaults, login names and passwords 52
delete command 50, 60, 88
device management commands 60, 88
Device Manager 34
device names, reserved 44
devices command 59
DHCP relay commands
global 197
port 198
VLAN 201
diagnostics 92
Differentiated Services 182
diffserv commands
configure 184
show 184
directory command 46, 61, 88
directory flags 46
Distance Vector Multicast Routing Protocol. See DVMRP commands
DVMRP commands
config 249
global 249
port 254
show 251
VLAN 256
Dynamic Host Configuration Protocol. See DHCP relay commands

E

eoc-mode 117
Ethernet port commands
configure 185
OSPF configure 232
OSPF show 234
show 186
VRRP 240

executable files 42
exit command 85

F

file management commands
Boot Monitor CLI 60
Run-Time CLI 88
file names 43
file system commands 45
files
configuration 42
executable 42
flags command 59
flash boot option 59
flash memory 40
format command 46, 61, 88

G

GUI (Graphical User Interface) 33

H

help command
boot 60
Boot Monitor CLI 62
Run-Time CLI 73, 81
history commands 62, 84

I

IGMP 168
IGMP snoop commands
configure 169
show 171
image files 42
Internet Group Management Protocol. See IGMP
Internet Group Management Protocol. See IGMP
Internet Packet Exchange. See IPX commands
IP addresses 75
IP ARP commands
configure 189
show 191
ip command, Boot Monitor CLI 63
IP commands
configure 178
show 180
IP DHCP commands
configure 197
show 197
IP diffserv commands
configure 184
show 184
IP DVMRP commands
show 251
ip filter commands 29
IP filters 294
IP flow commands 277
IP forwarding commands 180, 278
IP OSPF commands
configure 219
show 225–231
IP policies 279
IP policy commands
configure 279–289
show 289
IP RIP commands
configure 208
show 210
IP traffic-filter commands
configure 295–301
show 301
IP VRRP commands
port 241
show 246
IPX commands
RIP 268
SAP 270
set 267
show 272

static route 268
VLAN 266
IPX configuring 264
IPX RIP commands 268
IPX SAP commands 270

K

keystrokes, Run-Time CLI 72

L

l3 IP IGMP commands 257
layer 2 read-write security access 52
layer 3 IGMP commands
IP 257
port 260
show 258
VLAN 261
layer 3 read-write security access 52
link state database 230
log commands
Boot Monitor CLI 61
configure 106
show 107
log files 42
login command 85
login names, default 52
logout command 85

M

MAC address assignment 344
management commands
Boot Monitor CLI 60
Run-Time CLI 88
management tools 34
mirror commands 145
MLT commands
configure 146
show 148
monitor commands 305
Multi Link Trunking. See MLT commands
multicast commands 246

N

naming files 43
navigation commands 78
network boot option 59
network lists 281
NVRAM 44

O

Open Shortest Path First. See OSPF
OSPF accept policy 282
OSPF announce policy 284
OSPF commands
IP 219
port 232, 234
show 225
switch 220
VLAN 237

P

Passport Configuration Page 35
Passport models 33
password commands 104
passwords
default 52
levels 53
Run-Time CLI 71
PCMCIA boot option 59
PCMCIA cards 41
physical MAC address 346
ping command
Boot Monitor CLI 65
Run-Time CLI 85

pingipx command 86
port ARP commands
configure 193
show 193
port commands
configure 127–129, 185
layer 2 127
OSPF configure 232
OSPF show 234
show 129–139, 186
VRRP 240
port DHCP commands
configure 198
show 199
port DVMRP commands
configure 254
show 255
port IP VRRP commands 241
port l3 IGMP commands 260
port numbers 73
port OSPF commands
configure 232
show 234
port RIP commands
configure 211
show 214
port traffic-filter commands 301
port VRRP commands 242
ports, numbering 343
product support 32
publications
hard copy 31
related 29, 30

Q

quit command
Boot Monitor CLI 67
Run-Time CLI 85

R

RADIUS commands
configure 142
description 142
show 144
RADIUS configuration settings, displaying 144
Read/write access 52
Read/write/all access 52
Read-only access 52
recover command 51, 61, 88
reset command 59, 86
RFCs 30
RIP accept policy 286
RIP announce policy 287
RIP commands
IP 208
port 211
show 301
VLAN 215, 216
rlogin command 89
RMON commands
configure 109
show 109
Routing Information Protocol. See RIP
rsh command 88
Run-Time CLI
definition 69
description 70
help commands 73
IP address format 75
navigation 72
number supported 70
password and login levels 71
port number syntax 73
system requirements 70
using 71
Run-Time CLI commands
arp show 191
copy 88

- delete 88
- device management 88
- directory 88
- file management 88
- format 88
- history 84
- ping 85
- quit 85
- reset 86
- squeeze 88
- testing 92
- trace 94

run-time image files 42

S

save command 59

script file 80

script files, copying 91

security levels, descriptions 52

security, RADIUS 142

set dates 110

show cli commands 103

show commands, Boot Monitor CLI 59, 67

show config command 97

show log commands 107

show ports commands 129–139

show ports stats commands 248

show radius commands 144

show rip command 301

show sys commands 119

show tech command 100

show test commands 93, 94

show web-server command 126

Silicon Switch Fabric. See SSF

skip boot options 59

squeeze command 51, 61, 88

SSF 36

standby SSF module, accessing 92

station requirements
- Boot Monitor CLI 55
- Run-Time CLI 69

STG commands
- configure 150
- show 156

support, Nortel Networks 32

syntax command 71

sys set action commands 114

sys set commands 117

sys set flags commands 115, 116

syslog commands
- configure 123
- show 125

system commands 110

system flash memory 41, 43

T

technical publications 31

technical support 32

telnet command 88

test commands
- Boot Monitor CLI 59
- Run-Time CLI 92
- show 93

tests command 59

text conventions 28

TFTP 44

tftp command 60

trace commands 61, 94

trace log 43

traceroute command 87

traffic-filter commands
- port 301
- show 301

Type of Service 182

U

UDP commands
configure 204
show 205
UNIX 123
User Data Protocol. See UDP commands

V

virtual MAC address 347
Virtual Router Redundancy Protocol. See VRRP commands
VLAN ARP commands
configure 194
show 195
VLAN commands
config 157
configure forwarding database 165
configure IGMP snoop 168
show 161
show IGMP snoop 171
VLAN DHCP commands
configure 201
show 202
VLAN DVMRP commands
configure 256
VLAN IP commands 186
VLAN IPX commands 266
VLAN l3 IGMP commands 261
VLAN OSPF commands
configure 237
show 239
VLAN RIP commands 215, 216
VLAN VRRP commands
configure 244
show 245
VLANs, creating 157
VRRP commands
configure 240
show 245
VLAN 244

W

Web server commands 126
Web-based management 35
web-server commands
configure 126
show 126